

المعلوماتُ وجمالوتُ

المعارك الخفية لتجميع بياناتك
والسيطرة على عالمك

تأليف: بروس شنابر

ترجمة: د. أحمد مغربي

منشورات العلاقات العربية والدولية



المعلوماتُ وِجَالُوتُ

حين تضع هاتفك في جيبك كل صباح، أنت تعقد صفقة غير مُعلنة تقول: أريد أن أتبادل المكالمات مع الآخرين، وبالمقابل أسمح للشركة المصنّعة أن تعرف أماكن وجودي بدقة في كل الأوقات، ما يعني إبقائي تحت رقابتها الدائمة. إذا كان هاتفك ذكياً فهو عملياً حاسوب، وكل تطبيقاته تقدّم معلومات شخصية عنك، حين تستخدمه وحين لا تستخدمه. وإذا اتصلت بالإنترنت تتضاعف المعلومات عنك وعن أصدقائك وبرمجيّاتك وتعاملاتك وخياراتك فيما تشاهده وتسمعه وتقله، وفي نهاية المطاف، تفكر فيه.

لقد نشأت صناعة سمسة معلومات كاملة تتركّز حول التكبّب من بياناتك، تُباع فيها معلوماتك الشخصية، دون معرفتك ويدون إذن منك، إلى شركات مختلفة، تبعتها بدورها إلى متاجر ومراكز تسوّق سيعرف موظّفوها اسمك وعنوانك ومستوى دخلك بمجرد عبورك الباب، وتعرفك لوحات الإعلانات في الطرقات، ورفوف محلات البقالة، وتسجّل استجاباتك وتتعاون معاً لإغوائك باستهلاك المزيد. ويقود كل ذلك نموذج حوسبة جديد يجمع بياناتك الشخصية في "سحابة إلكترونية" تبقى هي أيضاً تحت سيطرة الشركات المصنّعة، ومن ورائها الحكومات.

لأول مرة في التاريخ الإنساني، كما تنبأ جورج أورويل روائياً، وكشف إدوارد سنودن فعلياً، تمتلك الحكومات القدرة على ممارسة رقابة شاملة ومنفلتة على شعوبها، داخل بلدانها وخارجها.

"كل مهتم بالحريّة والخصوصيّة والأمن في عصر الفضاء الإلكتروني يجب أن يقرأ هذا الكتاب".

جوزيف س. ناي الابن

السعر:

50 ريالاً قطرياً - 14 دولاراً

ISBN: 978-9927-103-80-3



9 789927 103803

مِنْبَذُ الْعِلَاقِ الْعَرَبِيَّةِ الدُّوَلِيَّةِ

هاتف: 44080451 +974 فاكس: 44080470 +974 صندوق بريد: 12231
الموقع الإلكتروني: fairforum.org البريد الإلكتروني: info@fairforum.org
العنوان: مبنى رقم 28، المؤسسة العامة للثقافة (كتارا)، الدوحة، قطر

المعلومات وجالوت
المعارك الخفية لتجميع بياناتك والسيطرة على عالمك



المعلومات وجالوت

المعارك الخفية لتجميع بياناتك والسيطرة على عالمك

تأليف

بروس شناير

ترجمة

د. أحمد مغربي



Bruce Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*, New York & London: W. W. Norton Company, 2015.
© Bruce Schneier 2015

عنوان الكتاب: المعلومات ورجالوت
المعارك الخفية لتجميع بياناتك والسيطرة على عالمك

تأليف: بروس شناير

ترجمة: د. أحمد مغربي

528 صفحة - 16.5 × 24 سم.

رقم الإيداع بدار الكتب القطرية: 2016/367

الرقم الدولي (ردمك): 978-9927-103-80-3 ISBN:

جميع الحقوق محفوظة لمنندى العلاقات العربية والدولية.

الطبعة الأولى 2017.

قيل في مديح كتاب المعلومات وجالوت:

«ثمة حاجة ماسة لكتاب المعلومات وجالوت. فبالإضافة إلى السيل الجارف من القصص المتواترة حول حروب الفضاء الافتراضي، واختراقات نُظُم المعلومات، والتجسس على الشركات، أثارت الأسرار التي كشف عنها [إدوارد] سنودن لدى كثيرين مشاعر الحيرة والمرارة حيال حماية خصوصيتهم الشخصية. يحدوني الأمل بأن كتاب بروس شنابير الجديد سوف يمكن عامة الناس من المشاركة في النقاشات، داخل المحاكم وخارجها، حول كيفية التفكير بجديّة ونزاهة في الوضع الراهن للرقابة الإلكترونية، والأهم من ذلك كيفية بناء مجتمع رقمي يقوم على قبول المحكومين ورضاهم».

سندي كوهن، المستشارة القانونية لـ «مؤسسة الحدود الإلكترونية»

«وضع بروس شنابير كتاباً مهماً يحمل رؤيةً ثاقبة إلى أبعد الحدود حول كيفية تأثير «البيانات الضخمة»، وابنة عمها «الرقابة العامة»، في حياتنا وما يمكننا فعله إزاءهما. على عادته، يأخذ شنابير أفكاراً ومعلومات فائقة التنوع والتعقيد، ويجعلها مفعمة بالحياة وسهلة الفهم ومقنعة لدرجة لا تقاوم».

جاك غولد سميث، الرئيس السابق لـ «مكتب الاستشارات

القانونية» في وزارة العدل إبان ولاية الرئيس جورج دبليو بوش

«الإنترنت حال من الرقابة التقنية، وكل تقنية، للرقابة استخدامات جيّدة وأخرى سيّئة. يستند بروس شنابير إلى مهاراته التاريخية والتقنية الواسعة للتمييز بين هذين الحدين، فيحلّل كلا التحديّ الذي تمثّله رقابة «الأخ الكبير»، ورقابة مجموعة «الإخوة الصغار». يتحتم على كل مهتم بالأمن، والحرية، والخصوصية، والعدالة في عصر الفضاء الافتراضي الذي نعيشه أن يقرأ هذا الكتاب».

جوزيف س. ناي الابن، أستاذ الخدمة المميّزة في

جامعة هارفرد، ومؤلف كتاب مستقبل السلطة

«يعتبر بروس شنابير الصوت الأكثر أتراناً وموثوقية وإطلاعا بشأن قضايا الأمن والخصوصية في زمننا. ويقدم الكتاب خبرة شنابير ومهاراته التحليلية الدقيقة لتقنية مهمة وسريعة التطور ولقضايا حقوق الإنسان المرتبطة بها. لقد قيل الكثير عن الطرق التي تعتمدها حكومتنا ومؤسساتنا المالية وهيئاتنا الشبكية في جمع المعلومات. في المقابل، لم يُقل سوى القليل عن كيفية استخدام ذلك المحيط اللامتناهي من المعلومات أو كيف يمكن استخدامه. في مواجهة مروحة واسعة من الخيارات الممكنة، والمغطاة بسحب السرية، يشكل كتاب بروس صوت المنطق المكين».

غزني جاردن، المؤلفة المشاركة للمُدونة الإلكترونية «بوينغ بوينغ»

«يشكل كتاب المعلومات وجالوت دليلاً لا غنى عنه لفهم التهديد الأبرز للحرية في المجتمعات الديمقراطية المرتكزة إلى حرية السوق. سواء يعترك القلق حول الرقابة الحكومية في عصر ما بعد سنودن، أم حول تلاعب شركتنا «فيسبوك» و«غوغل» بك، اعتماداً على المجموعات الهائلة من المعلومات لديها، فإن ما يكتبه شنابير الاختصاصي والرائد والمستقل حقاً عن هذه التهديدات المعاصرة، يقدم نظرة شاملة وغنية عن التقنيات والممارسات التي تقودنا صوب مجتمع الرقابة، والحلول المتنوعة التي يجب أن نلجأ إليها لإنقاذنا من ذلك المصير».

يوشاي بنكلر، أستاذ «بركان للدراسات القانونية الاستشارية»
في كلية القانون بجامعة هارفرد، ومؤلف كتاب ثروة الشبكات

«تعطي البيانات والخوارزميات والآلات المفكرة شركاتنا ومؤسساتنا السياسية قوى هائلة وواسعة التأثير. لقد أنجز بروس شنابير عملاً مميّزاً في تحليل تلك القوى وتأثيرها في خصوصياتنا وحياتنا ومجتمعنا. يجب أن يوضع المعلومات وجالوت على رأس قائمة كل شخص للكتب الواجب قراءتها».

أوم ماليك، مؤسس شركة «غيغوم»

الإهداء

إلى كارين في مركز «دي إم إيه إس سي» (DMASC)

المحتويات

11	مدخل
25	الجزء الأول
27	1 - المعلومات منتجاً جانبياً للحوسبة
39	2 - المعلومات بوصفها رقابة
59	3 - تحليل بياناتنا
81	4 - تجارة الرقابة
105	5 - الرقابة والسيطرة الحكوميتان
129	6 - تعزيز السيطرة المؤسسية
143	الجزء الثاني
145	7 - العدالة والحرية السياسية
169	8 - العدالة التجارية والمساواة
185	9 - التنافسية التجارية
195	10 - الخصوصية
209	11 - الأمن
235	الجزء الثالث
237	12 - المبادئ
253	13 - حلول للحكومة
285	14 - حلول للشركات

317 15 - حلول للبقية منا
335 16 - الأعراف الاجتماعية ومقايسة «البيانات الضخمة»
353 تنويهاات
361 الهوامش
511 الفهرس

المعلومات (*) وجالوت (**)

مدخل

إذا أردت أن تقتنع بأنك تعيش في عالم من الخيال العلمي، فما عليك سوى النظر إلى هاتفك الخلوي. إذ بات ذلك الجهاز الجذاب والأنيق والشارق القوة مركزياً في حياتنا إلى حد أننا أصبحنا نسلّم بداهةً بوجوده. يبدو أمراً طبيعياً تماماً أن تُخرج ذلك الجهاز من جييبك، بغض النظر عن مكان وجودك على كوكب الأرض، وتستخدمه للحديث مع شخص آخر، أيّاً كان موقعه على هذا الكوكب أيضاً.

لكن، في كل صباح تضع فيه الهاتف الخلوي في جييبك، أنت تعقد صفقة غير مُعلنة تقول: «أريد أن أبادل المكالمات بواسطة هاتف الخلوي، وبالمقابل أسمح للشركة التي تعطيني خدمات الاتصال أن تعرف أمكنة وجودي بدقة في كل الأوقات». لا تردّ تلك المقايضة في أي عقد، لكنها متأصلة في طريقة عمل خدمات الخلوي. الأرجح أنك لم تفكر بها من قبل، لكنك ربما صرت تفكر بها الآن بعد أن ذكرت لك، وقد تعتقد أنها صفقة جيدة. الهاتف الخلوي حقيقةً ابتكار عظيم، لكنه لا يعمل دون أن تعرف شركات الخلوي مكان وجودك دوماً، ما يعني أنها تبيّك تحت رقابتها المستمرة.

(*) في علوم الكمبيوتر، هناك فارق كبير بين مصطلحي بيانات (Data) ومعلومات (Information)؛ لأن المعلومات هي ما يستخلص من البيانات، لكن ورد المصطلحان غالباً في الكتاب كأنهما متشابهان. (جميع الحواشي السفلية للمترجم)

(**) لفظ "جالوت" (Goliath) وارد في القرآن الكريم ومستخدم في العربية الحديثة وبعض الكتب الدينية، مثله في ذلك مثل "غوليات".

هذا الشكل من الرقابة لصيق وحميمي جداً. إذ يتتبع الخلوي⁽¹⁾ أمكنة سكنك وعملك، والأمكنة التي تحب قضاء الأمسيات وعطل نهاية الأسبوع فيها. ويتتبع وتيرة ذهابك إلى الكنيسة (ويحدّد أي كنيسة)، والمدة التي تقضيها في «البار» [ويحدّد أي «بار»]، وما إذا كنت تسرع أثناء قيادتك السيارة في الطريق إليهما. وبحكم معرفته عن كل الهواتف الأخرى في منطقتك، يتتبع أيضاً الأشخاص الذين تقضي أيامك معهم، ومن تلتقيهم على وجبة الغداء، ومن تنام معهم. والأرجح أن تلك المعلومات المتراكمة⁽²⁾ تستطيع أن ترسم صورة عن كيفية قضاء وقتك بأفضل مما تستطيع أنت؛ لأنها ليست مضطرة للاستعانة بالذاكرة البشرية. في عام 2012، كان باستطاعة الباحثين⁽³⁾ استخدام هذه المعلومات لتوقع أين سيقضي الناس أوقاتهم في الـ 24 ساعة التالية، ضمن مسافة 20 متراً.

قبل الهواتف الخلوية، إذا رغب شخص ما في معرفة تلك المعلومات كلها، لربما وجب عليه أن يستأجر محققاً خاصاً كي يلاحقك باستمرار مسجلاً الملاحظات عنك. باتت تلك مهنة بالية الآن؛ إذ يقوم الخلوي المستقر في جيبيك بكل تلك الأمور أوتوماتيكياً. قد لا يستخرج أحد تلك المعلومات، لكنها موجودة بتصرف من يلتقطها.

المعلومات عن أمكنة وجودك قيمة، والكل يسعى للوصول إليها. الشرطة تريدّها؛ إذ يساعد تحليل المعلومات⁽⁴⁾ المكانية في التحقيقات الجنائية بطرق متنوّعة. وتستطيع الشرطة⁽⁵⁾ أن «ترن» على هاتف معيّن لتحديد مكانه، وتستعمل معلومات تاريخية لتحديد الأمكنة التي كان فيها قبل ذلك، وجمع كل «البيانات المكانية» عن الهواتف في منطقة معينة كي تعرف الأشخاص الذين كانوا فيها وأوقات وجودهم. أصبح رجال الشرطة يستخدمون معلومات الخلوي⁽⁶⁾ لتحقيق تلك الأهداف بصورة مطّردة.

وتستعمل الحكومات أيضاً المعلومات عينها من أجل التهيب والسيطرة الاجتماعية. في 2014، بعثت الحكومة الأوكرانية⁽⁷⁾ بالرسالة النصية التالية التي لا يخفى طابعها الأوروبي^(*): «عزيزي المشترك، جرى تسجيلك كمشارك في شغب جماعي». لا يذهب بك الظن بأن ذلك السلوك يقتصر على البلدان التي تحكمها نظم شمولية وحدها؛ ففي العام 2010، سعت شرطة ولاية «ميشغن»⁽⁸⁾ إلى الحصول على أرقام هواتف كل من تجمّعوا بالقرب من مكان إضراب عمالي متوقع، ولم تكثر بالحصول على مذكرة قضائية في ذلك الشأن.

هناك صناعة كاملة مكرسة للحصول على معلومات تتعقب أمكنة وجودك على مدار الساعة، وفي الوقت الحقيقي الجاري. وتستعمل الشركات هواتفك الخلوي⁽⁹⁾ لتتبع المخازن التي تتسوّق منها كي تتعرف إلى طريقتك في الشراء، وتتبعك في الطرقات كي تعرف إمكان وجودك قرب مخزن محدد، لترسل لك إعلاناً على الهاتف استناداً إلى البيانات عن أمكنة وجودك.

صارت «البيانات المكانية» قيمة جداً⁽¹⁰⁾، إلى حدّ أن شركات الخلوي باتت تبيعها إلى سيطرة المعلومات، الذين يبيعونها بدورهم إلى كل راغب في الدفع مقابل الحصول عليها. وتتخصّص شركات كـ «سينس نتوركس»⁽¹¹⁾ (Sense Networks) في صنع «بروفایل» شخصي عن كل منا، استناداً إلى ذلك النوع من المعلومات.

ليست شركات الخلوي المصدر الوحيد للمعلومات عن الهواتف. إذ تبيع شركة «فيرنت»⁽¹²⁾ (Verint) نظماً لتعقب الخلوي إلى شركات وحكومات في العالم كله. وعلى موقعها الشبكي⁽¹³⁾، تصف الشركة نفسها بأنها «رائد عالمي في حلول الذكاء العملائي لضمان الحدّ الأقصى من مشاركة العملاء، والأمن الاستخباراتي، ومنع الاحتيال والمخاطر وفرض التجاوب والإذعان»، مع زبائن لها في «ما يزيد على

(*) إشارة إلى رواية الكاتب جورج أورويل الشهيرة 1984 التي رسم فيها صورة مجتمع يجري التحكم به بواسطة رقابة مرئية - مسموعة مستمرة.

عشرة آلاف منظمة في أكثر من 180 بلداً. وتبيع شركة «كوبهام» (Cobham) البريطانية نظاماً يتيح إرسال مكالمات «عمياء» إلى أي هاتف خلوي⁽¹⁴⁾؛ بمعنى أنها لا تجعل الهاتف يرن، وليس بالمستطاع استشعارها. وترغم المكالمات العمياء الهاتف الذي يستقبلها على التجاوب معها بموجة ذات تردد معين، ما يجعل المرسل قادراً على تحديد مكان الخلوي المستقبل، ضمن مسافة لا تتعدى متراً واحداً. وتفاخر الشركة⁽¹⁵⁾ بأن لها زبائن حكوميين في الجزائر وبروناي وغانا وباكستان والسعودية وسنغافورة والولايات المتحدة. وتبيع شركة أخرى اسمها «دفيتك» (Defebtek)⁽¹⁶⁾، وهي مؤسسة غامضة مسجلة في جزيرة بنا، نظاماً معلوماتياً تقول الشركة إنه «يستطيع تحديد أرقام الهواتف في العالم بأسره وملاحقتها... من دون أن تشعر به شبكات الخلوي، ولا مقدمو خدماتها، ولا المتلقي». وليست تلك الكلمات مجرد تفاخر فارغ، فقد برهن الباحث في الاتصالات توبياس إنغل⁽¹⁷⁾ على الأمر نفسه في أحد مؤتمرات قرصنة الكمبيوتر («هاكرز»/ Hackers*) في العام 2008. ويفعل مجرمون كثر الأمر عينه حالياً.

تعتمد كل نظم التتبع المكاني هذه على النظام الخلوي. لكن هناك نظام آخر مختلف كلياً، وأكثر دقة في تحديد الأماكن، موجود في هاتفك الذكي: نظام تحديد المواقع جغرافياً في العالم، واختصاراً «جي بي إس» (GPS). إنه النظام الذي يوفر المعلومات المكانية للتطبيقات الرقمية المختلفة الموجودة على هاتفك. وتستخدم بعض تلك التطبيقات معلومات الـ«جي بي إس» في تقديم خدماتها، مثل «خرائط غوغل» (Google Maps)، و«أوبر» (Uber) و«يلب» (Yelp). فيما تسعى تطبيقات أخرى، مثل «أنغري بيردز» (Angry Birds)، إلى مجرد القدرة على تجميعها ثم بيعها⁽¹⁸⁾.

تستطيع أنت أيضاً فعل الأمر نفسه، فـ«هيلو سباي» (HelloSpy)⁽¹⁹⁾ تطبيق يمكنك تسريبه خفية إلى هواتف الآخرين الذكية كي تتبّع حاملها، وهو خيار مثالي

(*) هو المتمرّس بالكمبيوتر بما يمكنه من اختراق حواسيب الآخرين.

لأم قلقلة تود معرفة الأماكن التي يرتادها ابنها المراهق، أو لرجل سبي يرغب في التجسس على زوجته أو صديقته⁽²⁰⁾. كما استخدم بعض المديرين تطبيقات رقمية مشابهة للتجسس على موظفيهم⁽²¹⁾.

تستعمل وكالة الأمن القومي في الولايات المتحدة (US National Security Agency)، ونظيرتها البريطانية، «مركز قيادة الاتصالات الحكومية» (Government Communications Headquarters)، المعلومات المكانية لتتبع عامة الناس. وتجمع وكالة الأمن القومي البيانات المكانية للهواتف الخلوية⁽²²⁾ من مصادر متنوعة: أبراج الخلوي التي تتصل بها الهواتف، وشبكات الـ «واي-فاي» التي تدخل إليها، ومواقع الأمكنة التي تحددها تقنية الـ «جي بي إس» بواسطة تطبيقات الإنترنت. وتحتوي اثنتان من قواعد البيانات في وكالة الأمن القومي، تحملان اسمين حركتين هما «هاي فووت» (HAPPY FOOT) و«فاس- سي آي إيه» (FAS- CIA)، معلومات شاملة عن مواقع الهواتف عالمياً. وتستخدم الوكالة قواعد بياناتها لتتبع تحركات الناس، ورصد من يلتقون بأشخاص تهتم بأمرهم، وكذلك توجيه أهداف الطائرات من دون طيار («درون» / Drone).

يقال أيضاً إن وكالة الأمن القومي تستطيع تتبع الهواتف الخلوية حتى حين تكون مغلقة⁽²³⁾.

لم يطل حديثي حتى الآن سوى «البيانات المكانية» التي تجمع من مصدر واحد- جهازك الخلوي - لكن القضية أوسع من ذلك بكثير. الحواسيب التي تتعامل معها تنتج على الدوام معلومات شخصية حميمة عنك. وتتضمن ما تقرأه، وتشاهده، وتستمع إليه. وتشمل من تتحدث إليه، وما تقوله له. وتغطي في النهاية ما تفكر به، على الأقل بمقدار ما تقودك أفكارك إلى الإنترنت ومحركات البحث فيها. نحن فعلاً نعيش العصر الذهبي للمراقبة⁽²⁴⁾.

قالها سكوت ماكنيلي، الرئيس التنفيذي لشركة «صن مايكروسيستمز» (Sun Microsystems) بوضوح تام قبل زمن بعيد في عام 1999: «لديك صفر خصوصية⁽²⁵⁾ في كل الأحوال. انس الأمر». هو مخطئ بالطبع حول ردة فعلنا على الرقابة وما يجب عمله إزاءها، لكنه محق تماماً في أن الحفاظ على الخصوصية وتجنب الرقابة يغدوان أكثر صعوبة باطراد.

الرقابة مصطلح مثقل بالدلالات السياسية والعاطفية، لكنني أستعمله عامداً. إذ يُعرّف الجيش الأميركي الرقابة⁽²⁶⁾ بأنها «ملاحظة ممنهجة». وكما سأوضح، ينطبق ذلك التعريف تماماً على الرقابة الإلكترونية المعاصرة. نحن نُكُتَب مفتوحة بالنسبة للحكومات والشركات، وقدرتها على التمعن في حياتنا الشخصية الجمعية أضخم مما كانت عليه في أية فترة سابقة.

أكرر القول ثانية: إن الصفقة التي تجريها مع شركات متنوعة هي الرقابة مقابل الحصول على خدماتها الحرة. في كتابها المشترك العصر الرقمي الجديد (New Digital Age)، رسم إريك شميدت، رئيس شركة «غوغل»^(*)، ويارد كوهن، رئيس «قسم الأفكار» فيها، صورة تلك الصفقة. وهنا، أعيد صوغ رسالتهما: «إذا سمحت لنا بالحصول على جميع معلوماتك⁽²⁷⁾، فسوف نريك إعلانات ترغب في رؤيتها، وسنهبك مجاناً القدرة على البحث المفتوح في الإنترنت والبريد الإلكتروني وكل أنواع الخدمات الأخرى». إنه تبادل مصالح أساساً. نحن البشر حيوانات اجتماعية، ولا شيء يعادل مكافأتنا ويؤثر فينا كالتواصل مع الآخرين. باتت الوسائل الرقمية الطريقة الأسرع والأسهل في الاتصال. لكن لماذا نسمح للحكومات بالوصول إلى معلوماتنا؟ لأننا نخاف الإرهابيين، ونخاف أن يختطف الغرباء أطفالنا، ونخاف مهربي المخدرات، ونخاف الأشرار من كل نوع ومن آخر صنف رائج حالياً.

(*) تعرف تلك الشركة الآن باسم "ألفابت" (Alphabet)، وتسميتها «غوغل» رائعة.

إنّهُ التبرير الذي تقدّمه «وكالة الأمن القومي» لبرامجها في الرقابة العامة⁽²⁸⁾: إذا سمحت لنا بالحصول على معلوماتك كافة، فلسوف نتكفل بإزاحة الخوف عنك.

المشكلة أنّ تلك الصفقات ليست جيّدة ولا عادلة، على الأقل بالطريقة التي يجري ترتيبها اليوم. لقد درجنا على قبولها بسهولة زائدة، ومن دون أن نفهم حقاً بنودها وشروطها.

إليك ما هو حقيقي. إن التكنولوجيا الرقمية اليوم تعطي الحكومات والشركات قدرات جبارة على الرقابة العامة. والرقابة العامة خطيرة. فهي تمكّن التمييز استناداً إلى أية معايير تقريباً: العرق والدين والطبقة والمعتقدات السياسيّة. ويجري استخدام تلك الرقابة في السيطرة على ما نراه، وما نستطيع فعله، وبالنتيجة على ما نقوله. كما يجري استخدام تلك الرقابة من دون منح المواطنين أي حماية أو قدرة حقيقية على الاختيار أو الرفض، ومن دون وجود ضوابط وتوازنات كافية. إنّها تجعلنا أقل أماناً، وأقل حرية. والقوانين التي وضعناها لحمايتنا من هذه المخاطر في نُظم التقنيّات السابقة، صارت غير كافية إلى حد كارثي؛ بل إنّها غير فعّالة ولا تعمل. نحن بحاجة لإصلاح ذلك، وإصلاحه سريعاً جداً.

في الكتاب الحالي، أقيم تلك الحجّة في ثلاثة أجزاء.

يصف الجزء الأول مجتمع الرقابة الذي نعيش فيه. يدقّ الفصل الأول في أنواع المعلومات الشخصية التي نولدها أثناء حياتنا. ولا يقتصر الأمر على «البيانات المكانية» التي أتيت على ذكرها سابقاً في الهاتف الخلوي. هناك أيضاً المعلومات عن مكالماتنا الهاتفية العادية، وبريدنا الإلكتروني، ورسائلنا النصية القصيرة، إضافة إلى صفحات الإنترنت التي نقرؤها، والمعلومات عن معاملاتنا الماليّة، وأشياء كثيرة أخرى. لا يدرك معظمنا المدى الذي باتت فيها الحواسيب منبّئة في كل ما نفعله، أو الكلفة المتدنية لتخزين المعلومات على الكمبيوتر إلى حد جعل من الممكن حفظ

كل البيانات التي تتدفق منا إلى ما لا نهاية. كذلك يقلل معظمنا من السهولة التي صارت عليها عملية التعرف إلينا باستخدام معلومات نعتقد أنها طيّ الكتمان.

يُظهر الفصل الثاني كيف تستعمل كل تلك المعلومات لأغراض الرقابة. وكيف تحدث في كل مكان، بصورة أوتوماتيكية، من دون تدخل بشري، ويعيداً عن الأعين. إنها الرقابة العامة كلية القدرة.

من السهل التركيز على طريقة جمع المعلومات من قبل الحكومات والشركات، لكن ذلك يعطي صورة مشوهة. تكمن القصة الحقيقية في كيفية معالجة تلك السيول من البيانات، وربطها وتحليلها. وليس معلومات عن شخص بعينه، بل معلومات عن الجميع. الرقابة الشاملة تختلف جذرياً عن تجميع كثير من معلومات الرقابة الفردية، وتحصل على مدى لا نظير له من قبل. سأتحذث عن ذلك في الفصل الثالث.

تُجمع بيانات الرقابة بشكل رئيس من شركات نتعامل معها كزبائن أو مستخدمين. يتناول الفصل الرابع نماذج الرقابة التجارية، خصوصاً الإعلان المُشخصَن (Personalized Advertisement). لقد نشأت صناعة سمسة معلومات كاملة تركز حول التكبسب من بياناتنا، وتُباع فيها معلوماتنا الشخصية وتشتري دون معرفتنا وبلا إذن منا. ويقود ذلك حالياً نموذج جديد من الحوسبة، قوامه تجميع بياناتنا في «سحابة»، يجري الدخول إليها بواسطة أجهزة كـ«آي فون»، هي أيضاً تبقى تحت السيطرة اللصيقة للمُصنّع. وبالنتيجة، صارت الشركات تستطيع الوصول إلى معلوماتنا الأكثر حميمية والسيطرة عليها بشكل غير مسبوق.

يلتفت الفصل الخامس إلى قضية الرقابة الحكومية. كل حكومات العالم تفرض رقابة على مواطنيها، وتقتحم حواسيبهم محلياً ودولياً. ترغب الحكومات بالتجسس على الجميع للوصول إلى المجرمين والإرهابيين وكذلك -تبعاً لنوعية الحكومة- النشاط السياسي والمنشقين ونشطاء البيئة والمدافعين عن حقوق المستهلك

والمفكرين الأحرار. أركّز بشكل رئيس على «وكالة الأمن القومي» لأنها الوكالة الحكومية السريّة التي بتنا نعرفها أكثر من غيرها، بسبب تسرّب وثائق سنودن.

تتساوى الحكومات والشركات في امتلاك شهية لا تشبع لمعلوماتنا، وسأناقش كيف يعمل الطرفان معاً في الفصل السادس. أسّمي ذلك «شراكة القطاعين العام-الخاص في الرقابة»، وذلك تحالف عميق الغور. إنه السبب الرئيس في جعل الرقابة واسعة الانتشار، وإعاقتها محاولات إصلاح النظام.

كل هذه الأمور مهمّة، حتى لو كنت تثق بالشركات التي تتعامل معها والحكومة التي تعيش في ظلها. مع أخذ ذلك بالاعتبار، يتناول الجزء الثاني الرقابة العامة الشاملة، مبيّناً الأضرار التي تنجم عنها.

في الفصل السابع، أناقش الأضرار التي تنجم عن رقابة الحكومة. إذ بين التاريخ تكراراً الأضرار المتأتية من السماح للحكومة بممارسة رقابة عامة منفلة على مواطنيها. تشمل قائمة الأضرار المحتملة السيطرة على المواطنين والتمييز بينهم، والأثار المربعة على حرية التعبير والفكر، والإساءة الحتمية لاستخدام السلطة، وضياع الحرية والديمقراطية. تملك الإنترنت قدرة كامنة في أن تكون محرّكاً ضخماً للحرية والتحرّر عالمياً، لكننا نبدد تلك الإمكانيّة بالسماح للحكومات بممارسة رقابة عالميّة شاملة.

يلتفت الفصل الثامن إلى الأضرار الناجمة عن انفلات رقابة الشركات. إذ باتت الشركات حاضراً مُحكَم سيطرتها على «أمكنة» تجمّعنا على الإنترنت، وتُنقّب في المعلومات التي نتركها هناك، كي توظفها لمصلحتها. وبسماحنا للشركات بأن تعرف كل شيء عَنّا، فإننا نتيح لها أن تصنّفنا وتتلاعب بنا. يجري ذلك التلاعب في الخفاء ومن دون قوانين، وتزداد فعاليته مع تطوّر التقنية.

تؤدّي الرقابة الشاملة إلى أنواع أخرى من الأضرار. يبحث الفصل التاسع الاقتصادية منها، أساساً على الأعمال الأميركية، وهي تحدث عندما يحاول مواطنو

دول مختلفة حماية أنفسهم من رقابة وكالة الأمن القومي وحلفائها. تمثل الإنترنت منصة عالمية، وسوف تتسبب المحاولات التي تبذلها بلدان كالألمانيا والبرازيل لبناء جدران وطنية حول معلوماتها، بأضرار مكلفة للشركات التي تتيح للحكومات أن تمارس الرقابة، خصوصاً الشركات الأميركية.

في الفصل العاشر، أناقش الأضرار التي يتسبب بها ضياع الخصوصية. إن أنصار الرقابة - من وكالة الاستخبارات الألمانية الشرقية التي اشتهرت باسم «ستازي» (Stasi)، إلى ديكتاتور تشيلي السابق الجنرال أوغستو بينوشيه، إلى مدير «غوغل» إريك شميدت - اتكأوا دوماً على القول المأثور «إذا لم يكن لديك ما تخبئه، فليس لديك ما تخشاه». يجسد ذلك القول مفهوماً ضيقاً بشكل خطير لمفهوم الخصوصية. إذن الخصوصية هي حاجة إنسانية أساس، وهي مركزية لقدرتنا على التحكم بالطريقة التي نتفاعل بها مع العالم. والحرمان من الخصوصية يحط من إنسانية البشر بشكل أساسي، ويتساوى في ذلك أن يلاحقنا مخبر شرطة سري، أو أن ترصد جداول حسابات («خوارزميات» / Algorithms^(*)) في الكمبيوتر كل تحرك نأتي به.

في الفصل الحادي عشر، ألتفتُ إلى الأضرار التي تلحقها الرقابة بالأمن. غالباً ما تصوّر الرقابة الحكومية العامة باعتبارها مكسباً أمنياً، وشيئاً يحمينا من الإرهاب. على الرغم من ذلك، لم يقدّم دليل فعلي على نجاحات حقيقية للرقابة الشاملة حيال الإرهاب، في مقابل وجود أدلة مهمة على حدوث أضرار بسببها. الحال أن التمكن من ممارسة رقابة شاملة، يفرض الإبقاء على الإنترنت غير آمنة، ما يجعلنا جميعاً أقل أمناً تجاه الحكومات الأخرى المنافسة، وتجاه المجرمين وقراصنة الحواسيب («هاكرز»).

(*) التسمية مشتقة من اسم عالم الرياضيات محمد الخوارزمي، وهو مؤسس علم الجبر أيضاً. وتعمل الجداول الخوارزمية على تقديم حلول لمسائل رياضية معقدة بتبسيطها إلى خطوات متتالية يضبطها نظام معين للأرقام.

في الختام، يرسم الجزء الثالث ما يجب علينا فعله كي نحمي أنفسنا من رقابة الحكومات والشركات. إنَّ المعالجات معقّدة بقدر القضايا المتّصلة بالرقابة الشاملة، وتتطلب تنبهاً جيّداً للتفاصيل. مع ذلك، وقبل الدخول إلى التوصيات التقنية المحدّدة وتلك المتعلقة بالسياسات تجاه الرقابة، يقدّم الفصل 12 ثمانية مبادئ عامة توجه تفكيرنا في تلك المسألة.

يضع الفصلان التاليان توصيات محدّدة في مجال السياسة الواجب اتباعها، للحكومة (الفصل 13) وللشركات (الفصل 14). تتضمن بعض التوصيات تفاصيل أكثر من بعضها الآخر؛ ويميل بعضها لأن يكون طموحاً أكثر من كونه عملياً وقابلًا للتنفيذ. لكن كل التوصيات مهمّة، وقد تضر أية حذفات بالحلول الأخرى.

ينتقل الفصل 15 إلى ما يمكن لكل منا فعله فردياً. أقدم بعض النصائح التقنية المفيدة عملياً، بالإضافة إلى مقترحات لما يمكن فعله سياسياً. نعيش في عالم تستطيع التقنية فيه أن تغلب على السياسة، كما يمكن للسياسة أن تغلب على التقنية، لكننا نحتاج أن يعمل كلاهما معاً.

اختتم الفصل 16 بالتفكير في ما يمكن أن نفعله بصورة جماعيّة كمجتمع. تتطلّب معظم توصيات الفصلين 13 و 14 إجراء نقلة في طريقة فهمنا للرقابة وأهمية الخصوصية؛ لأننا لن نتوصل إلى إجراء إصلاحات قانونيّة مهمّة، من دون أن يطالب المجتمع بها. هناك فائدة كبرى من تجميع معلوماتنا لغايات البحث الطبي، وتطوير التعليم، ووظائف أخرى مفيدة للمجتمع. يجب أن نعرف كيف نستفيد من ذلك جماعيّاً، مع تقليص الأضرار. هذه هي القضية الأساس التي يركّز عليها إليها كل شيء في هذا الكتاب.

يشمل الكتاب أشياء كثيرة، ما يعني أن تغطيته سريعة بالضرورة. وتتضمّن الملاحظات الختاميّة مراجع موسّعة للمهتمين بالتعمق في الأمور. تتوافر تلك الملاحظات أيضاً على الموقع الشبكي للكتاب (www.schneier.com/dg.html).

تجد أيضاً في الموقع تحديثات للكتاب، اعتماداً على حوادث وقعت عقب انتهائي من كتابة مخطوطته.

أكتب بتحيز شديد للولايات المتحدة. إذ تأتي معظم الأمثلة من الولايات المتحدة، وتنطبق معظم التوصيات نموذجياً على الولايات المتحدة. ويرجع ذلك إلى أمر أساس هو أن الولايات المتحدة هي البلد الذي أعرفه. لكنني أعتقد أيضاً أن الولايات المتحدة تصلح مثلاً متفرداً عن الطريقة التي سلكت فيها الأمور مساراً خاطئاً، وهي في وضع متفرد لتغييرها نحو الأحسن.

خلفيتي في الأمن والتكنولوجيا. كتبتُ لسنوات طويلة عن كيفية تأثير التقنيات الأمنية في حياة الناس، والعكس بالعكس. راقبت صعود الرقابة في عصر المعلوماتية، ملاحظاً المخاطر الكثيرة وانعدام الأمن في هذا العالم الجديد. تعودت على التفكير في المسائل الأمنية، ونظرت إلى القضايا الاجتماعية الأوسع نطاقاً بعدسة المشكلات الأمنية. وقد منحني ذلك المنظور فهماً متفرداً للمشكلات والحلول معاً.

لست مناهضاً للتكنولوجيا، وليس الكتاب مناهضاً لها أيضاً. لقد جلبت الإنترنت، والعصر المعلوماتي عموماً، منافع ضخمة للمجتمع. وأعتقد أنها سيستمران في ذلك. لست حتى مناهضاً للرقابة. لقد ساهمت المنافع المتأتية من معرفة الكمبيوترات لما نفعله في إحداث تحول في الحياة بأسرها. أحدثت الرقابة ثورة في المنتجات والخدمات التقليدية، وأطلقت أنواعاً جديدة كلياً من التجارة، وصارت كذلك أداة لا تقدر بثمن في دعم القانون وإنفاذه. إنها تساعد شعوب العالم بطرق عديدة، وستستمر بفعل ذلك لفترة طويلة مستقبلاً.

لكن مخاطر الرقابة حقيقية، ولا نتحدث عنها بصورة كافية. ردة فعلنا على هذه الرقابة الزاحفة سلبية عموماً، فنحن لا نفكر بالصفقات التي نعقدها؛ لأن أحداً لم يضعها أمام أعيننا بوضوح بتلك الصيغة. تحدث التغيرات التقنية ونتقبل معظمها، ويصعب إلقاء

اللوم علينا، فالتغيرات تحدث بسرعة فائقة إلى حدّ أننا لم نقيّم حقاً تأثيراتها أو نوازن عواقبها. هكذا انتهينا إلى العيش في مجتمع الرقابة الذي تسلل خفية إلينا.

يجب ألا تكون الأمور على ذلك النحو، لكن علينا تولي الأمور بأنفسنا. يمكن أن نبدأ بإعادة التفاوض حول الصفقات التي نعقدها بمعلوماتنا. علينا أن نكون فاعلين في طُرُق تعاملنا مع التقنيات الجديدة. وعلينا التفكير في ما نرغب أن تكون عليه بنيتنا التحيّة تقنيّاً⁽²⁹⁾، وما القيم التي نرغب أن تجسدها. علينا أن نوازن أهمية معلوماتنا للمجتمع بطابعها الشخصي. وعلينا أن نتفحص مخاوفنا، ونقرر بكم من خصوصيتنا نحن مستعدون للتضحية مقابل راحتنا. علينا أن نتفهم الأضرار العديدة للرقابة المفرطة.

وعلىنا أن نقاوم.

منابوليس، ولاية مينوسوتا،

وكيمبردج، ولاية ماساتشوستس

تشرين الأول (أكتوبر) 2014

الجزء الأول

العالم الذي نصنعه

1

المعلومات منتجاً جانبياً للحوسبة

تنتج الحواسيب المعلومات بصورة مستمرة، فهي مُدخلاتها ومُخرجاتها. لكن المعلومات أيضاً منتج جانبي لكل ما تقوم به الحواسيب، التي توثق على الدوام كل ما تفعله في سياق عملياتها الاعتيادية، بل تحسّ وتسجّل أشياء تفوق إدراكنا لها.

يحتفظ برنامج معالجة الكلمات، مثلاً، بسجلّ عن كل ما تطبعه، بما في ذلك المسوّدات والتغيّرات في النصوص كلها. عندما تضغط على زر «حفظ»، يسجّل مُعالج الكلمات النسخة الجديدة، لكنه لا يمسح النسخ القديمة إلا إذا احتاج مساحة التخزين التي تحتلها كي ينجز عملاً آخر. كما يحفظ مُعالج الكلمات وثائقك أوتوماتيكياً على نحو متكرّر. برنامج «مايكروسوفت وورد» يحفظ وثائقي الخاصة كل 20 دقيقة، ويحتفظ بسجلّ عمن صنع تلك الوثائق، وغالباً كل من اشتغل عليها أيضاً.

اتّصل بالإنترنت، فيتضاعف إنتاجك للبيانات التي تشمل سجلات المواقع التي زرتها، والإعلانات التي نقرت عليها، والكلمات التي طبعتها. كذلك تُنتج المعلومات من حاسوبك، والمواقع التي زرتها، والحواسيب التي دخلت عليها عبر الشبكة. إذ يرسل برنامج تصفّح الإنترنت الذي تستعمله بيانات إلى المواقع الشبكية عن البرمجيات في حاسوبك، وتاريخ تثبيتها، والميزات التي فعلتها وما إلى ذلك. وفي

حالات عدّة، تكفي تلك المعلومات كي يجري التعرّف بدقة إلى حاسوبك⁽¹⁾ دون سواه.

صرنا نتواصل باطراد مع العائلة والأصدقاء والمعارف وزملاء العمل بواسطة الكمبيوترات، مستخدمين في ذلك البريد الإلكتروني، والرسائل النصيّة، و«فيسبوك» و«تويتر» و«إنستغرام» و«سناب شات» و«واتس آب» وكل ما هو دارج الآن. المعلومات نتاج فرعي لهذه الاجتماعية عالية-التقنية. ولا تكتفي هذه النُظم بنقل البيانات، بل تنشئ أيضاً سجلات للمعلومات عن مجريات تفاعلاتك مع الآخرين.

عندما تتمشى في الخارج، فلربما لا يخطر ببالك أنك تنتج معلومات، لكن الحال أنك تنتجها فعلياً. إذ يُجري هاتفك النّقال باستمرار حسابات حول مكان وجوده، استناداً إلى أبراج شبكة الخلوي القريبة منه. ليس الأمر أن شركة الخلوي تكثرث كثيراً بمكان وجودك، لكنها تحتاج إلى معرفة مكان هاتفك الخلوي كي تحوّل المكالمات إليه.

بالطبع، عندما تستخدم ذلك الهاتف فعلياً، فإنك تنتج مزيداً من المعلومات: الأرقام التي اتصلت بها واتصلت بك، والرسائل النصيّة التي أرسلتها وتلقيتها، ومدة المكالمات وما إلى ذلك. إذا كان هاتفك ذكياً، فهو حاسوب أيضاً، وكل تطبيقاتك تنتج معلومات حين تستخدمها - وحتى حين لا تستخدمها أحياناً. لربما احتوى هاتفك تقنية «جي بي إس» (GPS) (*) التي تنتج بيانات عن مكان وجودك، بدقة تفوق حتى ما تعطيه أبراج شبكة الخلوي. إذ تستطيع تقنية «جي بي إس» في هاتفك الذكي أن تحدّد موقعك بدقة تتراوح بين 16 و 27 قدماً (= بين 5.2 و 8.23

(*) تختصر عبارة «النظام الشامل لتحديد المواقع جغرافياً». ويرتكز عمل الـ «جي بي إس» على الاتصال مع سلسلة أقمار اصطناعية تستطيع تحديد مواقع الأشياء على الكرة الأرضية كلها.

متراً)، فيما تصل المسافة عينها إلى قرابة 2000 قدم (= 610 متراً) بالنسبة لأبراج الخَلوى.

اشتر شيئاً ما من متجر، وستُنتج مزيداً من المعلومات؛ إذ تمثل آلة المحاسبة نوعاً من الكمبيوتر يتولى صنع سجل عمّا اشترت، وتاريخ الشراء وزمنه. وتسري تلك المعلومات في شبكة الكمبيوتر الخاصة بالمتجر. وإذا لم تشتري بالمال نقداً، فلسوف تربط تلك المعلومات ببطاقتك الائتمانية. كذلك سترسل المعلومات إلى الشركة التي أعطتك تلك البطاقة، بل إن بعضاً من المعلومات سيظهر في قائمة حسابك الشهري فيها.

ربما احتوى المتجر أيضاً كاميرا فيديو للرقابة توضع بهدف تسجيل أدلة في حال حدوث فساد أو سرقة. وهناك كاميرا أخرى تصوّر كأميركا أثناء استخدامك آلة الصراف الآلي («إيه تي أم» / ATM). وهناك كاميرات أخرى تراقب المبانى والطُرق وعمرات المشاة والفضاءات العامة الأخرى.

اركب سيارتك، وستولّد مزيداً من المعلومات، إذ باتت السيارات الحديثة مكتظة بالحواسيب⁽²⁾ التي تولّد معلومات عن سرعتك، وقوة ضغط قدمك على الدوّاسات، ووضعيّة المقود وما إليها. تتجمّع معظم تلك البيانات بصورة أوتوماتيكية في الصندوق الأسود للسيّارة⁽³⁾، الذي يفيد في معرفة ما حصل أثناء حادث ما. حتى عجالات السيارة يحتوي كل منها حاسوباً لقياس الضغط فيها. وعندما تأخذ سيارتك إلى التصليح، فإنّ أول ما يفعله الميكانيكي هو الدخول إلى تلك المعلومات كلها كي يشخّص المشكلات. السيّارة ذاتيّة القيادة^(*) تولّد 1 غيغابايت من البيانات في كل ثانية⁽⁴⁾.

(*) يطلق التعبير على السيارات التي يقودها إنسان آلي (روبوت).

التقط صورة، وستدخل في عملية إنتاج المعلومات مجدداً؛ إذ تحتوي الكاميرا الرقمية بيانات عن تاريخ التقاط الصورة وزمانها ومكانها⁽⁵⁾ - نعم، تحتوي كاميرات عدّة تقنية «جي بي إس» - ومعلومات شاملة عن نوعها وعدساتها وإعداداتها، ورقم بطاقة هوية الكاميرا ذاتها. وعندما تضع الصورة على الـ «ويب»⁽⁶⁾، تبقى تلك البيانات مرتبطة بها.

لم تكن الأمور دوماً على ذلك النحو. في عصر الصحف والراديو والتلفزيون، كنّا نتلقى المعلومات دون وجود سجل عنها، بينما نتلقى الآن الأخبار والمواد الترفيهية بواسطة الإنترنت. اعتدنا طويلاً أن نتحدث إلى الناس وجهاً لوجه، ثم عبر الهاتف؛ فيما ينوب البريد الإلكتروني والمحادثات النصية عن ذلك حاضراً. واعتدنا أن نشترى الأشياء نقداً من المتجر، لكننا نستخدم الآن بطاقات الائتمان عبر شبكة الإنترنت. واعتدنا أن نستعمل القطع النقدية المعدنية في إجراء مكالمات من كشك الهاتف، والمروور بالباب الدوّار لمترو الأنفاق، وتشغيل عدّاد ركن السيارة قرب الرصيف. الآن، نستخدم نُظُمًا أوتوماتيكية للدفع، مثل «إيزباس» (EZPass)⁽⁷⁾، مرتبطة بأرقام لوحة السيارة وبطاقة الائتمان. كان الدفع لسيارة الأجرة نقداً بصورة حصرية في الماضي، ثم بدأنا ندفع ببطاقات الائتمان، وبتنا الآن نستخدم الهاتف الذكي للدخول إلى نظم شبكات سيارات الأجرة كـ «أوبر» (Uber) و«ليفت» (Lyft)، التي تصنع سجلات للمعطيات عن تعاملاتها، إضافة إلى مواقع صعودنا إلى التاكسي ونزولنا منها. وباستثناءات قليلة محددة، توجد الحواسيب الآن في كل أماكن التعامل التجاري ومعظم أمكنة لقائنا مع أصدقائنا.

في السنة الفائتة، حين تعطلت ثلاجتي استبدل رجل التوصيلحات الكمبيوتر الذي يديرها. أدركت حينها أنني كنت متخلفاً في نظرتي إلى الثلاجة: إنها لم تعد ثلاجة بكمبيوتر، بل كمبيوتر يقي على الطعام بارداً. وعلى غرار ذلك تماماً، تتحول الأشياء كلها إلى حواسيب. هاتفك كمبيوتر يجري مكالمات. وسيارتك

حاسوب بعجلات ومحرك. وفرنك حاسوب يخبز أطباق «اللاسانيه». وكاميرتك هي كومبيوتر يلتقط صوراً. حتى حيواناتنا المنزلية ومواشينا تُغرس فيها رقاقات إلكترونية بصورة منتظمة: قطتي عملياً كومبيوتر ينام في الشمس طيلة النهار.

كذلك صارت الكومبيوترات منبئة في المزيد من أنواع السلع المرتبطة بالإنترنت. هناك شركة اسمها «نست» (Nest) اشتراها محرك البحث «غوغل» بإيزيد على 3 بليون دولار في عام 2014، تصنع آلة ذكية مرتبطة بالإنترنت⁽⁸⁾ لتنظيم حرارة المنزل. وتعمل تلك الآلة على التأقلم مع عاداتك السلوكية من جهة، وتتفاعل مع ما يحدث مع شبكة الكهرباء العامة من الجهة الثانية. ولتتمكن من إنجاز ذلك، لا تكتفي تلك الآلة بتسجيل مقدار ما تستهلكه من الكهرباء، بل تنشئ سجلاً ثابتاً عن حرارة منزلك ورطوبته ومقدار الضوء المحيط، وما يتحرك قربة أيضاً. وبإمكانك شراء ثلاثة ذكية تحتفظ بسجل عن تاريخ صلاحية الأطعمة⁽⁹⁾، ومكيف هواء ذكي يرصد تفضيلاتك كي يرفع كفاءة الطاقة إلى حدّها الأقصى⁽¹⁰⁾. وهناك المزيد آت: تبيع «نست» الآن مجسّاً ذكياً⁽¹¹⁾ للدخان وثنائي أكسيد الكربون، وتخطّط لمجموعة كاملة من المجسّات المنزلية. كذلك تشتغل مجموعة كبيرة من الشركات على صنع مروحة واسعة من الأدوات الذكية. وسيكون ذلك ضرورياً إذا أردنا نشر شبكات كهرباء ذكية⁽¹²⁾ تستطيع خفض استهلاك الطاقة وانبعث الغازات الدفينة^(*).

نبدأ جمع المعلومات وتحليلها حول أجسادنا كوسيلة لتحسين صحتنا وعافيتنا. عندما ترتدي جهاز تتبّع اللياقة البدنية، كـ «فيتبت» (Fitbit) و«جوبون» (Jawbone)، فإنّه يجمع بيانات عن تحركاتك أثناء اليقظة والنوم، ثم يستعملها في تحليل عاداتك في التمرين والنوم، ويستطيع أن يحدّد متى تمارس الجنس⁽¹³⁾. كلما أعطيت ذلك الجهاز مزيداً من المعلومات عنك - كوزنك وغذائك - زادت إمكانية

(*) تشير التسمية إلى الغازات التي تلوث الغلاف الجوي للأرض وتسبّب في ظاهرة الاحتباس الحراري.

معرفتك⁽¹⁴⁾. وبالطبع، تلك المعلومات التي تشارك بها مع جهازك موضوعة على الإنترنت.

تبدأ مجموعة أدوات طبيّة بالتزوّد بالقدرة على دخول الإنترنت⁽¹⁵⁾، وهي تجمع مروحة من بيانات القياسات الحيوية، وتنشئ سجلات عنها. هناك للتو - أو سيكون هناك قريباً - أدوات تقيس باستمرار مؤشراتنا البيولوجية الأساسية، وأحوالنا المزاجية ونشاطات أدمغتنا. ولا يقتصر الأمر على الأدوات المختصة⁽¹⁶⁾، بل تحتوي الهواتف الذكية الحالية بعض المجسات الحساسة لقياس الحركة. ومع الانخفاض المتواصل في سعر تفكيك شيفرة الحمض النووي الوراثي «دي إن إيه» (DNA)، يعتمد المزيد منا إلى توليد المعلومات وتحليلها عن جينائنا. وتأمل شركات كـ«23 أند مي» (23andMe)⁽¹⁷⁾، في استعمال المعلومات عن جينات زبائنها للتوصل إلى تحديد الجينات المتصلة بالمرض، ما يقود إلى صنع علاجات مبتكرة ومريحة جداً. وتحدث تلك الشركات عن التسويق المُشخص⁽¹⁸⁾، وربما تشتري شركات التأمين ذات يوم ما جمعه تلك الشركات من معلومات⁽¹⁹⁾، لتستخدمها في التوصل إلى قرارات بشأن عملها.

لربما تتمثل الصورة القصوى لمسار التوليد الذاتي للمعلومات في صنع سجل لحياة الفرد⁽²⁰⁾ يعمل على التجميع المتواصل للمعلومات الشخصية. تتوافر للتو تطبيقات لصنع سجل حياة الفرد يمكنها تسجيل نشاطاتك على هاتفك الذكي، مثل الأوقات التي تحدث بها مع أصدقائك، أو تمارس الألعاب الرياضية، أو تذهب إلى السينما وغيرها. لكن ذلك لا يمثل سوى ظل باهت عما سوف تكونه سجلات الحياة. سوف تضم تلك التطبيقات مستقبلاً سجلاً بالفيديو⁽²¹⁾. وتعتبر نظارة «غوغل» أول أداة تقنية قابلة للارتداء تقدر على صنع سجل حياة بالفيديو⁽²²⁾، لكن هنالك عديدين يسعون للحاق بها.

هذه أمثلة عن «إنترنت الأشياء» (Internet of Things)⁽²³⁾. سوف ترصد مجسات بيئية مستويات التلوث. وستعمل نُظم التحكم وقوائم الجرد الذكية على خفض الهدر وتوفير المال. وسوف تدخل كوميوترات متصلة بالإنترنت في ثنايا الأشياء كافة - فيكون لدينا مدن ذكية⁽²⁴⁾، وفراشي أسنان ذكية⁽²⁵⁾، ومصابيح إنارة كهربائية ذكية⁽²⁶⁾، وأرصعة طرق ذكية⁽²⁷⁾، وزجاجات أدوية ذكية⁽²⁸⁾، وملابس ذكية⁽²⁹⁾ - ولم لا؟⁽³⁰⁾ تشير التقديرات حالياً إلى وجود 10 بلايين جهاز متصل بالإنترنت⁽³¹⁾. ويفوق الرقم للتو عدد سكان كوكب الأرض، بل إنني طالعتُ تقديرات تتوقع وصول الرقم إلى 30 بليوناً في العام 2020. مستوى النشاط⁽³²⁾ مرتفع جداً في هذا المجال، ولا نعرف الآن أي التطبيقات سيعمل وأياها سيفشل. ما نعرفه تماماً أننا جميعاً سنستمر في توليد معلومات، كميات هائلة من المعلومات. وسوف تضحى كل الأشياء التي تحيط بنا عيوناً وأذاناً للإنترنت⁽³³⁾.

تأثيرات كل هذه الاتصالية الشاملة على الخصوصية عميقة. كل تلك الأدوات الذكية ستخفض انبعاثات الغازات الدفيئة - لكنها ستضخّ أيضاً سيلاً من المعلومات عن الناس وتحركاتهم في منازلهم وكيف يقضون أوقاتهم. وسوف تجمع إشارات السير الذكية معلومات عن تحركات الناس خارج بيوتهم⁽³⁴⁾. لن تصبح الكاميرات إلا أفضل وأصغر وأكثر تحركاً⁽³⁵⁾. شركة «ريثيون» (Raytheon) (*) تعزم وضع منطاد صغير في سماء مدينتي واشنطن العاصمة وبالتيمور في عام 2015⁽³⁶⁾؛ لاختبار قدرتها على تتبّع «أهداف» - يفترض أنها عربات - في البر والبحر والجو.

في المحصلة، نحن نتفاعل مع مئات الكوميوترات يومياً، وسرعان ما سيرتفع عددها إلى الآلاف. كل واحد من هذه الكوميوترات ينتج معلومات، والقليل منها من النوع المثير: ما طلبناه في مطعم، أو معدل دقات قلبنا في هرولة المساء، أو

(*) تدرج شركة "ريثيون" ضمن الشركات السبع الكبرى المختصة في صنع الأسلحة للجيش الأمريكي.

آخر رسالة حبّ كتبناها. في المقابل، يندرج معظم تلك المعلومات ضمن ما يسمّى «ميتاداتا» أو بيانات حول البيانات («بيانات وصفية» / Metadata). والبيانات حول البيانات معلومات يستخدمها نظام كمبيوتر كي يعمل، أو معلومات تكون منتجاً جانبياً لعمل الحاسوب. في نظام رسائل نصيّة، تعدّ الرسائل نفسها معلومات، لكن الحسابات التي أرسلت الرسائل وتلقّتها، إضافة إلى زمنها وتوقيتها، هي كلها «بيانات وصفية» أو «ميتاداتا». يعمل نظام البريد الإلكتروني⁽³⁷⁾ على نحو مماثل، إذ تعدّ نصوص البريد الإلكتروني معلومات، لكن المعلومات عن المرسل والمتلقي ومسار الرسائل وأحجامها «ميتاداتا» - ويمكن الجدل حول كيفية تصنيف سطر المحتوى. في الصورة الفوتوغرافية، الصورة ذاتها معلومات؛ لكن تواريخها والرقم المتسلسل للكاميرا، ومعطيات إعداداتها، ومعلومات الـ «جي بي إس» عنها، هي - «ميتاداتا». قد تبدو الـ «ميتاداتا» غير مهمة، لكنها ليست كذلك البتة، وفق ما سأظهره لاحقاً.

استطراداً، لا تنجم تلك الغيوم من المعلومات التي نتجها بالضرورة عن خداع ومراوغة أي طرف. إذ يأتي معظمها ببساطة كمنتج جانبي طبيعي لعمل الحواسيب. هكذا تعمل التكنولوجيا حاضراً. البيانات هي «دخان عوادم»^(*) عصر المعلومات.

ما هي كمية المعلومات؟

إليك بعض الحسابات السريعة. ربما تكون سعة القرص الصلب في كمبيوترك المحمول 500 غيغابايت (Gigabyte). ولعلك اشتريت قرصاً صلباً احتياطياً لتخزين المعلومات بسعة 2-3 تيرابايت (Terabyte). وربما يكون القرص الصلب في الشبكة الداخلية لشركتك أكبر ألف مرّة من ذلك، أي بيتابايت (Petabyte). هنالك أسماء للأرقام الأكبر. إذ إن كل ألف بيتابايت تسمّى إكزابايت (Exabyte)⁽³⁸⁾،

(*) يشير التشبيه إلى الدخان الذي يصدر عن عوادم السيارات.

وهي تساوي بليون بليون بايت؛ وكل ألف إكزابايت تسمى زيتابايت (Zettabyte)، وكل ألف زيتابايت اسمها يوتابايت (Yottabyte). بتعابير بشرية، كل إكزابايت من المعلومات تساوي خمسمائة بليون صفحة من النصوص.

يتجمع «دخان عوادم» المعلومات مع بعضه بعضاً. بحلول عام 2010، كُتِبَ كجنس بشري نتج من المعلومات في اليوم الواحد أكثر مما أُنتجناه منذ بداية الزمن حتى عام 2003⁽³⁹⁾. وبحلول عام 2015، بات 76 إكزابايت من المعلومات تنقل عبر الإنترنت سنوياً⁽⁴⁰⁾.

عندما نبدأ التفكير بتلك المعلومات كلها، يبدو من السهل صرف النظر عن الانشغالات بشأن الاحتفاظ بها واستعمالها، بناءً على الافتراض بأن كميات المعلومات ببساطة أكبر من القدرة على تخزينها؛ وأن وفرتها الكبيرة في كل الأحوال تجعل من الصعب «غربلتها» للعثور على شذرات معلومات مفيدة. كان ذلك صحيحاً في الماضي. ففي مطالع العصر المعلوماتي، جرت العادة على التخلص من معظم تلك المعلومات - معظم «البيانات الوصفية» بالتأكيد - بعد وقت قصير من صنعها. بدا حينها أن تخزين تلك المعلومات يستلزم مساحات كبيرة من الذاكرة. لكن تكلفة مناحي الحوسبة كافة، انخفض بصورة مطردة مع مرور السنين، وما كان ينظر إليه قبل عقد بوصفه كميات معلومات ليس من العملي تخزينها ومعالجتها، صار أمراً يسهل التعامل معه اليوم. في العام 2015، بلغت تكلفة تخزين 1 بيتابايت من المعلومات في سحابة رقمية، قرابة مئة ألف دولار سنوياً⁽⁴¹⁾، ما يمثل هبوطاً بقرابة 90٪ عن المليون دولار التي كانت كلفة تخزينها في عام 2011. النتيجة تخزين المزيد والمزيد من المعلومات.

الأرجح أنك تستطيع تخزين كل تغريدة أرسلتها يوماً من محرك أقراص كمبيوترك المنزلي⁽⁴²⁾. فتخزين المكالمات الصوتية من هواتف الولايات المتحدة

كافة⁽⁴³⁾ يستلزم أقل من 300 بيتابايت، أو تكلفة 30 مليون دولار في السنة. ويتطلب تخزين سجل الحياة الشخصية في شريط فيديو 700 غيغابايت للفرد في السنة. إذا ضربت ذلك بعدد سكان الولايات المتحدة، يصل الرقم إلى 2 إكزابايت سنوياً، بتكلفة حالية تبلغ 200 مليون دولار. هذا مكلف، لكنه في متناول اليد، والسعر سينخفض باستمرار. في العام 2013، أكملت «وكالة الأمن القومي» تشييد قاعدتها الضخمة، «مركز يوتا للمعلومات» (Utah Data Center) في مدينة بلفيديل، وهو حالياً ثالث أكبر مركز معلومات في العالم⁽⁴⁴⁾، والأول في سلسلة مراكز بنيتها «وكالة الأمن القومي». التفاصيل سرية⁽⁴⁵⁾، لكن الخبراء يعتقدون أن «مركز يوتا» يستطيع تخزين 12 إكزابايت من المعلومات، وبلغت تكلفته حتى الآن 1.4 بليون دولار⁽⁴⁶⁾. على الصعيد العالمي، تستطيع مؤسسة «غوغل» تخزين 15 إكزابايت⁽⁴⁷⁾.

ما يصح على المؤسسات ينطبق على الأفراد أيضاً، وأنا نفسي مثال وحالة للدراسة. إذ يمتد تاريخ بريدي الإلكتروني إلى العام 1993، واعتبر ذلك الأرشفة البريدي جزءاً من دماغي. إنه ذكرياتي. لا يمر أسبوع دون أن أقلب ذلك الأرشفة بحثاً عن شيء ما: مطعم زرته قبل سنوات، مقال أخبرني أحدهم عنه، اسم شخص ما قابلته. وأنا أرسل إلى نفسي رسائل تذكيرية عبر الـ «إيميل» طيلة الوقت؛ لا يقتصر أمرها على أشياء يجب أن أنجزها عند عودتي إلى المنزل، بل أيضاً تذكيرات بأشياء قد أود استرجاعها بعد سنوات مستقبلاً. الوصول إلى ذلك المخزن وصول إلى كشخص.

اعتدت أن أفرز ذلك البريد بانتباه تام. يجب عليّ أن أقرر ما يجب حذفه أو الاحتفاظ به، وأعمد إلى إضافة الرسائل التي أقرر تخزينها مع مئات غيرها، في ملفات مصنفة وفق أسماء الأشخاص، والشركات، والمشاريع، وهكذا دواليك. في العام 2006، توقفت عن فعل ذلك، وأخزنت الرسائل كلها حالياً في ملف ضخمة، فمنذ عام 2006، صار التخزين والبحث بالنسبة لي أسهل من الفرز والحذف.

من أجل فهم ما يعنيه ركم كل تلك المعلومات للخصوصية الشخصية، يجدر التفكير بطالب الحقوق النمساوي ماكس شريمز. في العام 2011، طلب شريمز من موقع «فيسبوك» أن يعطيه كل ما يملكه من معلومات عنه⁽⁴⁸⁾. واستند طلبه إلى قوانين «الاتحاد الأوروبي». وبعد سنتين، وعقب منازعة في المحاكم، أرسل «فيسبوك» إلى شريمز أسطوانة مدججة («سي دي» / CD) تضم 1200 ملفاً من نوع «بي دي أف / pdf»⁽⁴⁹⁾. لم تقتصر محتويات الـ «سي دي» على كل الأصدقاء الذين يعرفهم، والأخبار التي تتبّعها، بل ضمت أيضاً كل الصور والصفحات التي نقر عليها، وكل الإعلانات التي رآها. شركة «فيسبوك» لا تستخدم تلك المعلومات كلها، لكن بدل أن تفرزها وتقرّر ما يجب الاحتفاظ به، وجدت الشركة أن من الأسهل الاحتفاظ بكل شيء.

2

المعلومات بوصفها رقابة

تعمل الحكومات والشركات معاً على تجميع المعلومات التي تنهمر منا في خضم حياتنا الرقمية وتخزينها وتحليلها. يجري ذلك غالباً من دون معرفة منا، ومن دون طلب موافقتنا. واستناداً إلى تلك المعلومات، تتوصل الحكومات والشركات إلى استنتاجات بشأننا، ربما لا نوافق عليها، أو حتى نحتج ضدها؛ لكنها تؤثر في حياتنا بطريقة عميقة. قد لا نحب أن نعرف بذلك، لكننا بتنا نعيش تحت رقابة واسعة.

يأتي كثير مما نعرفه عن «وكالة الأمن القومي»⁽¹⁾ من إدوارد سنودن، على الرغم من أن أشخاصاً عديدين، قبل سنودن وبعده، سرّبوا أسراراً عن الوكالة. وبوصفه متعاقداً مع «وكالة الأمن القومي»، جمع سنودن عشرات الآلاف من الوثائق تتضمن توصيفاً لنشاطات رقابية تمارسها. وفي عام 2013 فرّ سنودن إلى هونغ كونغ، وأعطى وثائق لصحافيين انتقامهم بنفسه. لفترة من الزمن، عملت مع غلين غرينوالد وصحيفة الغارديان البريطانية على تحليل وثائق من سنودن غلب عليها الطابع التقني.

برزت الأخبار الأولى عن مسألة سنودن متضمنة وصفاً للطريقة التي دأبت بها «وكالة الأمن القومي» على جمع بيانات عن سجلات مكالمات الأميركيين الخلوية⁽²⁾. إحدى الحجج التي دافعت بها الحكومة عن نفسها في نبرة تكررت كثيراً في أوقات لاحقة⁽³⁾، تمثلت في القول إنّ ما جمعته الوكالة كان مجرد «بيانات وصفية». تسعى

تلك الحجة إلى القول إن الوكالة لا تجمع الكلمات التي نقولها لبعضنا بعضاً بواسطة الخلوي⁽⁴⁾، بل تكفي بالبيانات عن أرقام الهواتف، وتاريخ المكالمات، وتوقيتها ومدتها. بدا أن ذلك قمين بتهدة الناس، لكن الأمور لم تجر على ذلك النحو. الحال أن جمع الـ «ميتاداتا» عن الناس يعني وضعهم تحت الرقابة⁽⁵⁾.

يمكن إقامة البرهان على بطلان تلك الحجة بواسطة تدريب ذهني بسيط. تخيل أنك استأجرت مخبراً خاصاً كي يتنصت على شخص ما. سوف يزرع المخبر لواقط سرية في منزل ذلك الشخص، ومكتبه، وسيارته. سوف يتنصت أيضاً على هاتف ذلك الشخص وكومبيوتره. وسوف يزودك بتقرير عن مكالماته.

تخيل الآن أنك طلبت من المخبر وضع ذلك الشخص تحت الرقابة. سوف تحصل على تقرير مختلف لكنه يبقى شاملاً إذ يضم الأمكنة التي يتردد عليها ذلك الشخص، وما الذي يفعله، وما هي مشترياته. تلك هي «البيانات الوصفية».

إذاً، التنصت يوصلك إلى كلام المحادثات الهاتفية، أما الرقابة فتعطيك كل شيء آخر.

تكشف «البيانات الوصفية» للهواتف وحدها أشياء كثيرة عنا. إذ تظهر مدة المكالمات وتكرارها وأوقاتها علاقتنا مع الآخرين: أصدقاءنا الحميمين، وزملاء العمل، وكل من يقع بين هاتين الفئتين. وتتكفل «البيانات الوصفية» للهواتف⁽⁶⁾ بكشف من هم الأشخاص الذين نهتم بأمرهم، وطرق اهتمامنا بهم، وما هي الأشياء التي نعتبرها مهمة، مهما كانت خصوصيتها. تفتح تلك المعلومات نافذة تطل على شخصياتنا⁽⁷⁾، وتقدم ملخصاً تفصيلياً عن ما يحصل معنا في الأوقات كلها⁽⁸⁾.

في تجربة أجرتها «جامعة ستانفورد»، جرى تجميع «البيانات الوصفية» لهواتف 500 متطوع على مدار بضعة شهور. وتفاعاً حتى الخبراء أنفسهم بمدى الطابع الشخصي الذي استطاعوا بلوغه في استنتاجاتهم المستندة إلى «ميتاداتا» هواتف المشاركين⁽⁹⁾. يستأهل التقرير عن تلك التجربة الاقتباس:

• اتّصل المشارك (أ) بمجموعات محلية مهتمة بالأمراض العصبية، وبصيدلية مختصة، وبخدمة رعاية مرض نادر، وب«خط ساخن» مع شركة أدوية مختصة حصرياً بعلاج مرض «التصلّب اللويحي المتعدّد» (Multiple Sclerosis) والمرتكس.

• تحدّث المشارك (ب) طويلاً مع مختصّين في أمراض القلب يعملون في مركز طبي كبير، وتحدّث باقتضاب مع مختبر طبي، وتلقّى مكالمات من صيدلية، وأجرى مكالمات قصيرة مع «خط ساخن» لمركز يقدم تقارير عن جهاز طبي يستعمل لرصد «اضطرابات نبضات القلب».

• أجرى المشارك (ت) عدداً من المكالمات مع متجر لبيع الأسلحة مختص بتجارة البنادق نصف الآلية من نوع «إيه آر»، كما تحدّث طويلاً مع مركز خدمة الزبائن لأحد منتجي تلك البنادق.

• اتصل المشارك (ث) على امتداد ثلاثة أسابيع مع محل لتصليحات المنازل، وصانع أقفال، ومركز مختص بالزراعات المائية^(*)، ومتجر لبيع أدوات تستعمل في تعاطي مواد الكيف.

• أجرت المشاركة (ج) اتّصلاً صباحياً طويلاً مع أختها. وأجرت بعد يومين سلسلة مكالمات مع موقع محلي لتنظيم الأسرة، ثم أجرت اتصالات أخرى قصيرة بعد أسبوعين، واتصلاً أخيراً بعد شهر.

استناداً إلى خط «بيانات وصفية» واحد، خلص الباحثون إلى أن المشاركين كانوا على التوالي: مريضاً يعاني «التصلّب اللويحي المتعدّد»، ومصاباً بنوبة قلبية، ومالك بندقية حربية نصف آلية، وزارعاً منزلياً لحشيشة الكيف، وامرأة أجرت إجهاضاً.

(*) زراعة منزلية غالباً لا يستعمل فيها التراب.

تعدُّ عمليات البحث عن المعلومات على الإنترنت مصدراً آخر للمعلومات الحميمية التي يمكن استعمالها في الرقابة⁽¹⁰⁾. (تستطيع المجادلة طويلاً إن كانت تلك بيانات أم «بيانات وصفية». تزعم «وكالة الأمن القومي» أن تلك البيانات هي «ميتاداتا»⁽¹¹⁾؛ لأن مكونات البحث متضمنة في روابط إلكترونية ضمن صفحات الإنترنت ومواقعها). نحن لا نكذب على محرك البحث، إذ تربطنا به علاقة أشد حميمية من تلك التي تربطنا بأصدقائنا، وأحبتنا، وأفراد عائلتنا. ونحن دوماً نخبره بما نفكر، وبأوضح ما يمكن من كلمات. يعرف «غوغل» جيداً نوع الـ «بورنو» الجنسي الذي يبحث عنه كل منا، وأياً من الأحبة القدماء ما زال في بالنا، وما نخجل منه، وما نهجس به، وما نبقيه سراً. إذا عقد «غوغل» العزم، فيأمكنه أن يعرف أياً منا قلقاً على صحته العقلية-النفسية، أو مهتماً بالتهرب من الضرائب، أو يخطط للاحتجاج ضد سياسة حكومية معينة. اعتدت القول إن «غوغل» يعرف ما أفكر به أكثر من زوجتي، لكن ذلك لا يذهب بعيداً بما يكفي، فـ «غوغل» يعرف ما أفكر به أكثر مما أعرف أنا؛ لأنه يتذكر الأشياء كلها بوضوح وإلى الأبد.

أجريت تجربة سريعة لخاصية الاستكمال التلقائي في محرك البحث «غوغل». وتمنح تلك الخاصية إمكان أن يستكمل «غوغل» في الزمن الحقيقي ما بدأت كتابته في خانة البحث، استناداً إلى ما كتبه آخرون في السابق. عندما كتبت: «هل يجب أن أخبر (w) ...»⁽¹²⁾، استكمل «غوغل» العبارة، فكتبت: «هل يجب أن أخبر زوجتي أنني أقمت علاقة غرامية؟» و«هل يجب أن أخبر عملي حول قيادتي السيارة تحت تأثير (الكحول أو المخدرات)؟» كتب «غوغل» ذلك لأنها العبارتان الأكثر شيوعاً بين جمهور مستخدميه. و«غوغل» يعرف كل الأشخاص الذين نقروا على استكمال إحدى العبارتين، إضافة إلى كل الأشياء الأخرى التي بحثوا عنها يوماً⁽¹³⁾.

(*) قد يشير حرف (w) بالإنكليزية إلى الحرف الأول في كلمة زوجة (wife) أو عمل (work)، ولذلك اختار برنامج الاستكمال التلقائي الإجابتين الواردتين في المثال.

في عام 2010 اعترف إريك شميدت، المدير التنفيذي لـ «غوغل»⁽¹⁴⁾، بأننا «نعرف أين أنت، ونعرف أين كنت، ويمكننا أن نعرف تقريباً ما تفكر به».

إذا كان لديك حساب في البريد الإلكتروني «جي ميل» (G-Mail)، يمكنك أن تتأكد من الأمر بنفسك. إذ تستطيع أن تعرف الأوقات التي دخلت فيها على ذلك البريد، منذ لحظة إنشاءك حسابك عليه، وربما لسنوات طويلة. افعل ذلك، وسوف تصاب بالدهشة. إنه أشد حميمية مما لو كنت أرسلت لـ «غوغل» مفكرتك الشخصية. وعلى الرغم من أن «غوغل» يتيح لك التحكم بالإعلانات التي ترغب في مشاهدتها، فأنت لا تملك الحق في حذف أي شيء لا ترغب به على حسابك في «جي ميل».

ثمة مصادر أخرى للمعلومات الحميمة و«البيانات الوصفية». فالسجلات عن عاداتك في التسوق تستطيع أن تكشف أشياء كثيرة عنك تكون. وتعلن تغريداتك على «تويتر» للعالم موعد استيقاظك صباحاً⁽¹⁵⁾، وموعد إيوائك إلى الفراش ليلاً. كما تكشف لوائح أصدقائك عن ميولك السياسية وخياراتك الجنسية⁽¹⁶⁾. وتخبّر عناوين رسائل بريدك الإلكتروني عن محلّ مركز القلب في حياتك المهنية والاجتماعية والعاطفية⁽¹⁷⁾.

إحدى الطرق للتفكير في تلك المواضيع تتمثل في النظر إلى المعلومات باعتبارها محتوى، فيما «البيانات الوصفية» هي سياق ذلك المحتوى. تستطيع الـ «ميتاداتا» أن تكشف أكثر مما تفعله المعلومات نفسها، خصوصاً إذا جُمعت وصُنّفت. عندما تضع شخصاً تحت الرقابة، تفوق أهمية محتويات المكالمات الهاتفية والرسائل النصية والبريد الإلكتروني ما تمتلكه «البيانات الوصفية». لكن، عندما تفرض الرقابة العامة، تكون الـ «ميتاداتا» هي الأكثر دلالة وأهمية وفائدة⁽¹⁸⁾.

كما قال ستيفوارت بيوكر، المستشار العام السابق لوكالة الأمن القومي، من المؤكّد أنه «باستطاعة «البيانات الوصفية» أن تخبرك كل شيء تماماً عن حياة شخص ما»⁽¹⁹⁾.

إذا كان لديك ما يكفي من الـ «ميتاداتا»، فأنت لا تحتاج عملياً إلى المحتوى»⁽²⁰⁾. وفي 2014، علّق مايكل هايدن، المدير السابق لـ «وكالة الأمن القومي» و«وكالة الاستخبارات المركزية» (CIA) قائلاً: نحن نقتل الناس اعتماداً على الـ «ميتاداتا»⁽²¹⁾. الحقيقة أن الفارق بين المعلومات و«البيانات الوصفية» وهمي إلى حد كبير؛ فكلاهما معلومات عتّا.

رقابة أرخص

تاريخياً، كانت الرقابة صعبة ومكلفة. كنا نلجأ إليها فقط حين يكون الأمر مهماً: عندما تحتاج الشرطة لتعقب مشتبه فيه، أو عندما تبحث شركة تجارية معينة عن سجل مفصل لتاريخ المشتريات لأغراض تتعلق بفواتيرها. كان هنالك استثناءات، وهي متطرفة ومكلفة. حكومة ألمانيا الشرقية المريضة إلى حد استثنائي بجنون الارتياب جندت 102 ألف شخص في صفوف جهاز الاستخبارات «ستازي»، لمراقبة مجموع السكان البالغ 17 مليون نسمة، بمعدل جاسوس لكل 166 مواطناً⁽²²⁾، أو جاسوس لكل 66 مواطناً إذا أضفت إلى الحساب المخبرين المدنيين. تطوّرت رقابة الشركات من جمع القليل الضروري إلى جمع كل ما يمكن من المعلومات. في الماضي كانت الشركات دائماً تجمع معلومات عن زبائنهم، لكنها لم تجمع الكثير منها، واحتفظت بها بمقدار ما كان ذلك ضرورياً. شركات بطاقات الائتمان كانت تجمع المعلومات فقط عن معاملات زبائنهم المالية التي تحتاجها لأغراض الفواتير. والمتاجر بالكاد جمعت معلومات عن زبائنهم، فيما لم تجمع شركات شحن البضائع بالبريد سوى الأسماء والعناوين، وربما مع شيء من تاريخ المشتريات كي تعرف متى ترفع اسم أحدهم من قوائمها البريدية. حتى «غوغل» عند بداياته الأولى، لم يجمع سوى القليل من البيانات عن مستخدميه، بالمقارنة مع ما يملكه منها اليوم. عندما كانت معلومات الرقابة مكلفة الجمع والتخزين، اكتفت الشركات بأقل ما يمكن منها.

انخفضت تكلفة تقنيات الحوسبة بصورة سريعة في العقود الأخيرة. كان ذلك أمراً جيداً إلى حد بعيد. أصبح من الأرخص والأسهل للناس التواصل ونشر أفكارهم والوصول إلى المعلومات وما إلى ذلك. لكن، في الآن ذاته، انخفضت تكلفة الرقابة. ومع التحسّن المطرد في تقنيات الكمبيوتر، صار بمقدور الشركات جمع المزيد من المعلومات عن كل من تتعامل معه. ومع انخفاض تكاليف تخزين المعلومات، استطاعت الشركات حفظ المزيد من المعلومات لزمن أطول. وإذا صارت أدوات تحليل البيانات الضخمة أشد قوة، بات تجميع مزيد من المعلومات أمراً مجزياً تماماً. أدى ذلك إلى ظهور نماذج الأعمال المستندة إلى الرقابة، على نحو ما سأحدث عنه في الفصل الرابع.

انتقلت رقابة الحكومة من العمل على جمع المعلومات عن أقل عدد ضروري من الأشخاص، إلى تجميعها عن أقصى عدد ممكن منهم. عندما كانت الرقابة يدوية ومكلفة، كان من الممكن تبريرها في الحالات القصوى وحدها. فضرورة الحصول على مذكرة تفتيش قلصت رقابة الشرطة، كذلك عملت محدودية الموارد ومخاطر الانكشاف على تقليص رقابة الاستخبارات على مستوى الدولة. استهدفت الرقابة أشخاصاً بعينهم، وجمعت أقصى المعلومات عنهم وحدهم. كما وُجِدَت قوانين صارمة تقلص إلى أدنى الحدود إمكان جمع المعلومات عن الآخرين. على سبيل المثال، عندما كان «مكتب التحقيقات الفيدرالية» (إف بي آي / FBI) (*) يترصد هاتف أحد رجال العصابات، كان يفترض بمسرق السمع وقف التسجيل وإغلاق الساعة فوراً عندما يدخل على الخط أولاد الشخص أو زوجته.

مع تطوّر التقنية وانخفاض تكلفتها، وسّعت الحكومات نطاق الرقابة. تستطيع «وكالة الأمن القومي» الآن أن تراقب مجموعات كبيرة - الحكومة الروسية، والطواقم الدبلوماسية الصينية، والمنظّمات السياسيّة اليساريّة ونشطاءها - وليس مجرد أفراد.

(*) يتولى مكتب التحقيقات الفيدرالي ("إف بي آي") شؤون الاستخبارات الداخلية في أميركا.

وتعني إمكانية مراقبة المكالمات الصادرة عن الهواتف الجواله إعطاء الـ «إف بي آي» قدرة التنصّت على الناس⁽²³⁾ بغض النظر عن الجهاز الذي يستعملونه في التواصل. وبالنتيجة، تستطيع وكالات الاستخبارات الأميركية التجسس على شعوب بأكملها، وتخزين بيانات عنها لسنوات طويلة. وترافق ذلك مع تغيير في طبيعة التهديد، فقد استمرت تلك الوكالات في التجسس على حكومات معينة، فيما وسّعت رقابتها الشاملة على مجاميع عريضة بحثاً عن أفراد يحتمل أن يكونوا خطيرين، وسأتحدّث عن ذلك في الفصل الخامس.

نتيجة لذلك، تلاقت مصالح الرقابة لدى الحكومات والشركات معاً. إذ بات كلاهما راغباً في معرفة كل شيء عن كل شخص. تتباين دوافع الطرفين⁽²⁴⁾، لكن المنهجيات نفسها، وهو السبب الرئيس للشراكة الأمنية القوية بين القطاعين الحكومي والخاص، التي سأتناولها في الفصل السادس.

لمعرفة ما أقصده بتكلفة تكنولوجيا الرقابة، يكفي النظر إلى أدوات التجسس المتقدمة والرخيصة التي يحصل عليها الزبائن العاديون. فثناء رحلة جوية، رُحْتُ أقلّب صفحات مجلة سكاي مول (Sky Mall)، وهي «دليل سلع» تحرص الخطوط الجوية على وضعه في خلفية مقاعد المسافرين في الرحلات الجوية المحلية في أميركا. لقاء 80 دولاراً، هناك قلم مع كاميرا خفية ومايكروفون، يمكنني من تسجيل وقائع أي اجتماع أرغب في الإبقاء على دلائل عنه لاحقاً. وبإمكاني أن أشتري كاميرا خفية مثبتة في راديو - ساعة، لقاء 100 دولار، أو كاميرا تعلق على حائط الغرفة على هيئة مستشعر للحركة. وأستطيع أن أضبط الكاميرتين كي تسجّلا ما يجري في الغرفة بصورة متواصلة، أو عندما تستشعران حركة فيها. وتتيح لي أداة أخرى الوصول إلى البيانات في الهواتف⁽²⁵⁾ - سواء أكانت «آي فون» (iPhone) أو «أندرويد» (Android) - بمجرد أن تكون في متناولي فعلياً. ويوضح الإعلان عن تلك الأداة أنها تمكّن من «قراءة الرسائل النصية حتى بعد حذفها. ورؤية الصور، ولوائح الاتصال، وتواريخ المكالمات، ومواعيد الروزنامة، والمواقع الإلكترونية

التي جرى الدخول إليها، وحتى الدخول إلى بيانات تحديد المواقع جغرافيا (GPS) في الهاتف لمعرفة الأماكن التي زارها». ولا يتجاوز السعر 120 دولاراً.

من محلات أخرى، أستطيع بأقل من 50 دولاراً شراء مسجل لوحة المفاتيح⁽²⁶⁾، أو مسجل المفاتيح، لمعرفة ما يطبعه شخص على لوحة مفاتيح حاسوبه بمجرد وصله مباشرة بالكمبيوتر. ومقابل قرابة 100 دولار، أستطيع الحصول على برنامج يمكنني من اعتراض مكالمات هاتفية لشخص قريب مني، والتنصت عليها⁽²⁷⁾. كذلك أستطيع بأقل من ألف دولار شراء طائرة «درون- هليكوبتر» تحمل كاميرا⁽²⁸⁾ ويمكن التحكم بها عن بُعد، كي أتجسس على جيراني.

إن الأدوات التي ذكرتها في تناول المستهلك، على الرغم من أن بعضها محظور في بعض الدوائر القانونية. كذلك تتجه أدوات الرقابة المحترقة لأن تكون أرخص سعراً وأكثر تطوراً⁽²⁹⁾. بالنسبة للشرطة، يغير انخفاض الأسعار كل شيء. إذ يكلف تتبع شخص ما خفية، سواء سيراً على الأقدام أم بالسيارة، قرابة 175 ألف دولار شهرياً -معظمها رواتب للعملاء القائمين بعملية التتبع. لكن، إذا استطاع رجال الشرطة دس متتبع إلكتروني في سيارة المشتبه فيه، أو استخدام برج زائف لاتصالات الخلوي بهدف مخادعة هاتف المشتبه فيه كي يرسل «المعلومات المكانية» إلى الشرطة مباشرة، تنخفض تكلفة الملاحقة إلى 70 ألف دولار شهرياً؛ لأنها لا تتطلب سوى عميل واحد. وإذا استطاعت الشرطة أن تخبي مستقبل إشارات الـ «جي بي إس» في سيارة المشتبه فيه، تنخفض التكلفة فجأة إلى قرابة 150 دولاراً في الشهر، معظمها تكلفة دس تلك الأداة خلسة في السيارة. ويفوق تلك الوسائل كلها رخصاً الحصول على معلومات عن أمكنة المشتبه فيه من مزود هاتفه الخلوي، وشركة «سبرينغ» (Spring) تقدّم تلك البيانات لقاء 30 دولاراً شهرياً.

يكنم الفارق بين التكاليف الثابتة والهامشيّة. إذا قام قسم شرطة برقابة مباشرة⁽³⁰⁾ سيراً على الأقدام ستكون تكلفة تتبع شخصين ضعفي رقابة شخص

واحد. لكن الرقابة بواسطة الخلوي أو نظام الـ «جي بي إس»، تكلف أساساً ما يستلزمه تثبيت النظام، وحالما يتم ذلك يصبح الفارق هامشياً وضيئلاً بين رقابة شخص واحد أو عشرة أشخاص أو ألف شخص. على نحو مماثل، بعد الإنفاق على تصميم وبناء نظام تنصّت على الهواتف يجمع الأصوات ويحلّلها في أفغانستان، كما فعلت «وكالة الأمن القومي» للمساعدة في حماية الجنود الأميركيين من المتفجرات محلية الصنع، يصبح من السهل وبسعر زهيد توظيف النظام التقني عينه للتنصّت على شبكات الهواتف في بلدان أخرى.

الرقابة العامة

لا يؤدي الانخفاض المستمر في تكلفة تقنيات الرقابة إلى مجرد فارق في السعر، بل إلى فارق نوعي أيضاً. إذ ينتهي الأمر بالمنظمات إلى ممارسة رقابة أكبر - أكبر بكثير. عقب قرار من «المحكمة العليا» الأميركية عام 2012، مثلاً، طُلب من مكتب التحقيقات الفيدرالي الحصول على مذكرات قضائية بشأن 3 آلاف جهاز تتبع بواسطة الـ «جي بي إس»، أو إغلاقها فوراً⁽³¹⁾. ببساطة، كان يستحيل على الـ «إف بي آي» تتبع 3 آلاف سيارة من دون اللجوء إلى الوسائل الإلكترونية المؤتمتة؛ فالوكالة ليست لديها قوة عاملة كافية لإنجاز تلك المهمة. حاضراً، مع انتشار الخلوي، أصبح من الممكن ملاحقة كل شخص، كل الوقت.

مثال آخر تقدمه المساحات الضوئية للوحات ترخيص السيارات، وهي أجهزة تزداد شيوعاً باطراد. إذ يحتفظ عدد من الشركات بقاعدة بيانات عن لوحات رخص السيارات التي تخلف أصحابها عن دفع قروض مركباتهم. هناك كاميرات مثبتة فوق سيارات الملاحقة وشاحنات الجّرّ، تعمل بصورة متواصلة على مسح لوحات رخص المركبات السائرة على الطرق، وإرسال البيانات إلى الشركات بحثاً عن المتخلفين. ومع وجود أموال كثيرة كامنة في تجارة إعادة تملك المركبات⁽³²⁾، ينخرط في العملية أشخاص كثر - ويرسلون جميعهم معلومات تصب في قواعد بيانات مركزية عند

الشركات. زعمت إحدى شركات الملاحقة، اسمها «فيجيلانت سوليوشنز أوف ليفرمور» (Vigilant Solutions of Livermore) ومقرها كاليفورنيا، أنها تمتلك 2.5 بليون سجل⁽³³⁾، وتجمع 70 مليون صورة مسح رقمي للوحات السيارات شهرياً، مع معلومات عن التاريخ والوقت والموقع وفق نظام الـ «جي بي إس».

إضافة إلى تجارة إعادة تملك السيارات⁽³⁴⁾، تباع شركات القارئ الضوئية معلوماتها إلى محامي الطلاق والمحققين الخاصين، وغيرهم. تبث تلك الشركات بياناتها أحياناً مباشرة إلى أقسام الشرطة التي تعمل على ربطها مع معلومات المسح الآتية من مداخل الطرق السريعة، ومراكز دفع رسوم المرور على الطرقات الرابطة بين الولايات، ونقاط عبور الحدود، ومواقف السيارات في المطارات. وتبحث الشرطة عن مركبات مسروقة، وسائقين صدرت بحقهم مذكرات قضائية، ومخالفات غير مدفوعة. يضاف إلى ذلك أن الـ «إف بي آي» دأبت على الاستفادة من قواعد المعلومات عن رخص القيادة⁽³⁵⁾ للتعرف إلى الأشخاص؛ وعملت «وزارة الأمن الوطني» على توحيد تلك المعلومات كلها في قاعدة بيانات موحدة على المستوى الوطني⁽³⁶⁾. في المملكة المتحدة، هناك قاعدة بيانات مماثلة⁽³⁷⁾ تستند إلى كاميرات الرقابة الثابتة المنشورة في طول البلاد وعرضها. وتدعم تلك البيانات إنفاذ نظام لندن لضريبة ازدحام المرور^(*)، والعثور على المركبات المتأخرة عن الاختبارات الإلزامية لصلاحية سيرها على الطرقات⁽³⁸⁾.

يجدر بك أن تتوقع حدوث أمر مماثل مع انتشار تقنية التعرف المؤتمت إلى الوجوه⁽³⁹⁾. في البداية، الأرجح أن تستعمل الصور التي تلتقطها الكاميرات الرقمية الخاصة من قبل حاصدي المكافآت، الذين يتتبعون أثر المتهرين من الكفالات القضائية. مع ذلك، ستباع تلك الصور في النهاية لاستخدامات أخرى ثم تصل إلى الحكومة. تملك الـ «إف بي آي» للتو قاعدة بيانات تحتوي 52 مليون وجه⁽⁴⁰⁾، مع

(*) يفترض بالمركبات عدم المرور في وسط لندن بين أول النهار وآخره، معظم الأسبوع، وتغرم المركبات المخالفة.

برامج كفاءة في التعرف المؤتمت إلى الوجوه. وتستخدم شرطة دبي حالياً نظاماً⁽⁴¹⁾ يستند إلى التكامل بين برامج التعرف إلى الوجوه وبين «نظارة غوغل»^(*) (Google Glass) للتعرف أوتوماتيكياً على المشتبه فيهم. ومع توفر أعداد كافية من كاميرات الرقابة في المدينة، سيتمكن ضباط الشرطة من ملاحقة السيارات والناس في كل مكان، من دون مغادرة مكاتبهم.

هذه هي الرقابة العامة، المستحيلة من دون كومبيوترات، وشبكات، ونظم أتمتة. وليس شعارها «لاحق تلك السيارة»، بل «لاحق كل سيارة». كان باستطاعة الشرطة دوماً تعقب من تشتبه به، لكن بوجود شبكة من الكاميرات في المدن، ومساحات لوحات السيارات، وبرامج التعرف إلى الوجوه، تستطيع الشرطة الآن تعقب الجميع - سواء مشتبه فيهم أم لا.

على نحو مشابه، كانت عملية شبك أداة اسمها «سجل القلم» على خط الهاتف الأرضي لمشتبه فيه، بهدف تسجيل الأرقام التي يتصل بها، مكلفة ومستهلكة للوقت. أما الآن فتستطيع «وكالة الأمن القومي» الحصول على تلك المعلومات من قواعد البيانات لشركات الهاتف⁽⁴²⁾، بل تستطيع الحصول على معلومات عن كل شخص في الولايات المتحدة. وقد فعلت ذلك.

في العام 2008، استحدثت شركة «وييز» (Waze) - التي استولت عليها شركة «غوغل» عام 2013 - نظاماً جديداً لتتبع الأمكنة على الهواتف الذكية. وتتلخص فكرته في أن الشركة تستطيع استعمال المعلومات المتأتمتة من رصد تحركات السيارات التي تستخدم نظام «وييز»⁽⁴³⁾ في استخلاص بيانات مرورية في زمن حقيقي، وتوجيه الناس صوب أسرع الطرق وأقلها ازدحاماً. بالطبع، كلنا نرغب في تجنب اختناقات المرور، وفي الحقيقة لا يستفيد مستخدمو نظام «وييز» وحدهم بل المجتمع

(*) نظارة تربط بكومبيوتر صغير يقدم معلومات عما يشاهده مرتديها، ويتدخل في المشاهدة نفسها أيضاً، بحذف غير المرغوب رؤيته وإضافة العكس.

برمته عندما يُبعد الناس عن الطرق المختنقة مرورياً فلا يزايدون في تفاقم المشكلة. لكن، هل نعرف كمية المعلومات التي نفرط بها ونقدّمها لذلك النظام؟

لأول مرة في التاريخ، تمتك الحكومات والشركات القدرة على ممارسة رقابة عامة على شعوب بأكملها. ويمكنها فعل ذلك عبر استخدامنا الإنترنت، واتصالاتنا الهاتفية، وتعاملاتنا المالية، وتحركاتنا... وكل ما نفعله. حتى الألمان الشرقيون لم يستطيعوا تعقب كل شخص كل الوقت، في حين أصبح ذلك سهلاً الآن.

رقابة خفية

إذا كنت تقرأ هذا الكتاب على جهاز «كيندل» (Kindle) للقراءة الإلكترونية⁽⁴⁴⁾، فليسوف تعرف ذلك فوراً شركة «آمازون» (Amazon) التي تصنعه. ستعرف «كيندل» متى بدأت القراءة، وكم كانت سرعتك فيها، وما إذا كنت قرأت الكتاب بشكل متواصل، أم كنت تكتفي بقراءة بضع صفحات منه يومياً، وإذا كنت قفزت إلى نهايته، ثم عدت ثانية لتقرأ أحد الفصول، وإذا وضعت علامات على إحدى الصفحات. وسوف تعرف شركة «آمازون» كل ذلك أيضاً. لا تلتمع أي إشارة ضوئية، ولا يظهر أي مربع حوار يحذرك بأن «كيندل» يرسل إلى «آمازون» معلومات عن عاداتك في القراءة، بل يحدث الأمر هكذا ببساطة، وبهدوء واستمرارية⁽⁴⁵⁾.

نحن نتساهل حيال مستوى من الرقابة الإلكترونية على الإنترنت لا نقبل به في العالم الفعلي، لأنه ليس واضحاً ولا معلناً. فأن يطلب منك موظف إبراز بطاقة هويتك، أو أن تلتقط كاميرا كشك المرور صورة اللوحة المعدنية لسيارتك، أو أن يطلب جهاز الصراف الآلي («إيه تي إم / ATM») بطاقتك مع الرقم الخاص بالشريحة الإلكترونية لتلك البطاقة، أمر مختلف عن الرقابة. صحيح أن كل تلك الأفعال تنتج سجلات رقابة⁽⁴⁶⁾ - والحالة الأولى قد تتطلب أن ينسخ الموظف أو يستولي بطريقة ما على المعلومات المذكورة في بطاقة هويتك - لكنها على الأقل حالات واضحة. نحن نعرف أنها تحصل.

معظم عمليات الرقابة الإلكترونية لا تحصل على تلك الشاكلة، فهي سرّية. نقرأ الصحف على الإنترنت دون أن ندرك أن المقالات التي قرأناها مسجلة. ونفتش في المخازن الإلكترونية دون أن نعرف أن كلا الأشياء التي نشترها وتلك التي نشاهدها ونقرر ألا نشترها قيد المراقبة المستمرة. ونستخدم نُظم الدفع الإلكترونية دون أن نفكر في كيفية احتفاظها بسجلات عن مشترياتنا. ونحمل هواتفنا الخلوية معنا دون أن نفهم أنها باستمرار تتعقب المواقع التي نكون فيها.

«بزفيد» (Buzzfeed) موقع شبكي للترفيه، يجمع كمّيات ضخمة من المعلومات عن مستخدميه. تأتي معظم تلك المعلومات من الطُّرق التقليديّة في تعقب الناس على الإنترنت، لكن «بزفيد» يحتوي كثيراً من المسابقات المرحّة يطرح بعضها أسئلة شخصيّة جداً. أحد تلك الأسئلة هو: «ما مدى حظوتك الاجتماعيّة؟»⁽⁴⁷⁾، ويطلب تفاصيل عن وضعك المالي، واستقرارك الوظيفي، ونشاطاتك الترفيهية، وصحتك العقلية - النفسية. دخل ما يزيد على مليوني شخص تلك المسابقة⁽⁴⁸⁾، دون أن يتنبهوا إلى أن «بزفيد» يخزن المعلومات من أسئلته ومسابقاته. وعلى نحو مُشابه، تجمع مواقع المعلومات الطبيّة كـ «ويب ميد» (WebMD)⁽⁴⁹⁾ معلومات عن الصفحات التي يفتش القراء عنها والتي يقرؤونها.

كي لا تظن أن المعلومات المتأتية من المواقع الشبكيّة التي تزورها، وبريدك الإلكتروني، ومكالماتك الهاتفية، و«غرف المحادثة»، وغيرها من وسائل الاتصال الإلكتروني تخضع وحدها للمراقبة، فإن الرسائل البريدية الورقية قديمة الطراز تخضع أيضاً للمراقبة. بواسطة برنامج اسمه «آيسوليشن كونترول أند تراكينغ» (Isolation Control & Tracking)، تصوّر «خدمة البريد الأميركي» الوجه الخارجي الأمامي والخلفي، لكل رسالة بريد ورقية في الولايات المتحدة. يشكّل ذلك قرابة 160 بليون قطعة سنوياً⁽⁵⁰⁾. وتتوافر تلك المعلومات لقوى إنفاذ القانون، وبالتأكيد لوكالات حكوميّة أخرى.

بعيداً عن الإنترنت، هناك عدد كبير من تقنيات الرقابة التي تغدو أصغر حجماً وأقل وضوحاً للعيان. في بعض المدن، تلتقط كاميرات الفيديو صور وجوهنا مئات المرات يومياً. بعضها بارز للعيان تماماً، لكننا لا نستطيع رؤية الكاميرات من نوع «سي سي تي في / CCTV» المثبتة قرب ضوء في السقف، أو صراف آلي (إيه تي أم)، أو كامير «غيبابكسل» فائقة القوة تراقبنا من عمارات سكنية مجاورة. كذلك تصغر أحجام طائرات الـ «درون» باطراد وتضحى أكثر خفاءً عن العيون⁽⁵¹⁾؛ فقد بلغ بعضها الآن حجم الحشرات، وسرعان ما ستصير بحجم ذرات الغبار.

إذا أضفت برامج التعرف الإلكتروني إلى نُظم جمع الصور، فسوف تحصل على نظام مؤتمت للرقابة الشاملة كاملة القدرة. تعتبر برامج التعرف إلى الوجوه الطريقة الأسهل لتحديد الأشخاص في صور الكاميرا⁽⁵²⁾، وتزداد هذه التقنية تطوراً سنة بعد أخرى. في عام 2014، صارت الخوارزميات الرقمية في التعرف إلى الوجوه أكثر اقتداراً من البشر⁽⁵³⁾. هنالك نظم أخرى للتعرف إلى الصور قيد التطوير: أجهزة لمسح قزحية العين تعمل عن بُعد⁽⁵⁴⁾، ونُظم التعرف إلى طريقة المشي⁽⁵⁵⁾، وهكذا دواليك.

ثمة تزايد في عمليات الرقابة في الشوارع. إذ يمكن تعقب الناس باستخدام نظام «التأشير بموجات الراديو» [يعرف باسمه المختصر «رفيد» (RFID) (*)]⁽⁵⁶⁾ وهو موجود في بطاقات الهوية والبطاقات الائتمانية التي تحملها في محفظتك. تتعقب مجموعة من المخازن الكبرى الناس بطريقة خفية⁽⁵⁷⁾، عبر التقاط ما تبثه بانتظام هواتفهم النقالة، سواء بنظام الـ «ماك» في الـ «آي فون» أم الـ «بلوتوث»، وهي تتكوّن أساساً من أرقام تلك الهواتف. يسعى ذلك التعقب إلى معرفة الأقسام التي يرتادونها، والرفوف التي يتوقفون عندها⁽⁵⁸⁾، والبضائع التي يتفحصونها وما إلى

(*) - يتكوّن من سلسلة من الخطوط القصيرة المرصوفة، وهي ترسل موجة راديو خفيفة، كذلك التي تستقبلها الآلات الحاسبة في المخازن، فتعرف إلى أسعارها.

ذلك. ويمكن تعقب عامة الناس أثناء مشاركتهم في مناسبات عامة بواسطة هاتين المقاربتين⁽⁵⁹⁾.

في 2014، أخبر مسؤول تنفيذي كبير في شركة «فورد موتور» الجمهور في «معرض الإلكترونيات الاستهلاكية»: «نعرف كل من ينتهك القانون، ونعرف متى تنتهكونه. لدينا أجهزة «جي بي إس» في سياراتكم، لذا نعرف ما تفعلونه». كان لذلك التصريح وقع الصدمة والدهشة، إذ لم يعرف أحد من قبل أن «فورد» تخضع مالكي سياراتها لرقابة مستمرة. سرعان ما سحبت الشركة التصريحات، لكن تلك التعليقات أفسحت المجال لكثير من التقلقل بشأن جمع «فورد» معلومات عن مالكي سياراتها⁽⁶⁰⁾. وبفضل تقرير صدر من «مكتب المحاسبة الحكومية»⁽⁶¹⁾، بتنا نعرف أن شركات صناعة السيارات وصناعة أدوات الملاحة الأرضية تجمع بيانات مواقع كثيرة من مستخدميها.

هناك رادارات بنطاق تردد «تيراهيرتز»⁽⁶²⁾ تستطيع اكتشاف أسلحة مخبأة يحملها الناس، وأشياء وأجسام عبر جدران اسمنتية تزيد سماكتها عن 8 إنشات [20 سنتيمتراً تقريباً]. وهناك كاميرات تستطيع «استراق السمع» على مكالمات هاتفية بالتركيز على أشياء قريبة من المتحدث⁽⁶³⁾، كأكياس البطاطا المقلية، وقياس الذبذبات الصادرة عنها. وتستطيع «وكالة الأمن القومي»، ونظرياً المؤسسات المشابهة، أن تشغل هاتفك الخلوي عن بُعد، وأن تصغي إلى ما يحدث حولك⁽⁶⁴⁾.

ثمة من يعمل على تطوير نُظم للتعرف إلى رائحة الأجساد أيضاً⁽⁶⁵⁾. وهناك شركة على الإنترنت تسعى إلى التعرف إلى الناس من طريقة طباعتهم على لوحة المفاتيح⁽⁶⁶⁾ وأسلوبهم في الكتابة⁽⁶⁷⁾. وتحصد الحكومات والشركات معاً عشرات الملايين من البصمات الصوتية⁽⁶⁸⁾، التي تمثل طريقة أخرى في التعرف إليك مباشرة في الوقت الفعلي.

ذلك هو المستقبل. سوف يعرف الموظفون في المتاجر اسمك، وعنوانك، ومستوى دخلك بمجرد عبورك الباب⁽⁶⁹⁾. وسوف تعرفك لوحات الإعلانات في الطرقات، وتسجل استجابتك لها⁽⁷⁰⁾. وسوف تعرف رفوف محلات البقالة ما تشتريه عادة⁽⁷¹⁾، وكيف يمكن إغراؤك بشراء مزيد من البضائع. وسوف تعرف سيارتك ركبها⁽⁷²⁾، ومن يقودها، وقوانين المرور التي يتقيد بها السائق وتلك التي يتجاهلها. حتى الآن، يبدو ذلك وكأنه خيال علمي.

مع تلاشي الرقابة في خلفيّة الأشياء، يصبح من الأسهل تجاهلها. وكلما ازداد تطفل نظام رقابة وفضوله، ازدادت أرجحية أن يكون خفياً. يرفض كثيرون منا إجراء «اختبار مخدرات» قبل توظيفهم، لكن العديد من الشركات يجري تحقيقات موسعة تسبر خلفيات موظفيها المحتملين كافة. على نحو مماثل، نشعر حين نكون موضع رقابة من مئات الشركات على الإنترنت - وهي شركات لم نتعامل معها ولا حتى سمعنا بها - بقدر أقل من التدخلية مقارنة بمئة باحث تسويق يلاحقونا باستمرار، ويسجلون ملاحظات عنا.

بمعنى ما، نعيش في حقبة فريدة من التاريخ؛ فالعديد من نظم الرقابة ما يزال مرئياً لنا. طُرُق التثبّت من الهوية شائعة، لكنها ما تزال تطلب منا إبراز بطاقة هويتنا. وتنتشر الكاميرات في كل الأمكنة، لكننا ما نزال قادرين على رؤيتها. في المستقبل القريب، ولأن تلك النظم ستغدو خفيّة، ربما ندعن دون معرفة منا إلى قدر حتى أكبر من الرقابة.

الرقابة المؤتمتة

يطالنا كم مدهش من الرقابة بصورة أوتوماتيكية، حتى لو بذلنا ما في وسعنا للخروج من دائرتها. ويجري ذلك لأننا نتفاعل مع الآخرين، وهم أنفسهم قيد المراقبة.

مع أنني لم أضع قط تدويناً على «فيسبوك» ولم أصادق أحداً فيه - إذ أملك صفحة مهنية لا حساباً شخصياً - فإن «فيسبوك» يتعقبني⁽⁷³⁾. في قاعدة بياناته، يحتفظ بملفات فيها «بروفایل» شخصي لمن لا يستعملون «فيسبوك». يلاحقني كلما دخلت صفحة على «فيسبوك» فيها زر «أعجبني» («لايك» / Like). والأرجح أنه يستطيع أن يخمن بصواب كبير من هم أصدقائي⁽⁷⁴⁾، استناداً إلى التذييلات الملحقة بصوري معهم، وربما لديه أيضاً «بروفایل» شخصي عني ملحقاً بمعلومات أخرى اشتراها من سماسرة المعلومات. ومع وجود أصدقاء لي على «فيسبوك»، وتلك المواقع التي تتضمن أزرار «أعجبني»، متاح له مراقبتي.

أحاول تجنب استخدام محرك البحث «غوغل»⁽⁷⁵⁾، لكن ذلك لا يحول دون قدرته على جمع المعلومات عن المواقع التي أزورها؛ لأن عدداً كبيراً منها يستعمل أداة «غوغل للتحليلات» (Google Analytics) في تتبع زوارهم. مرة أخرى، تتيح تلك المواقع لـ «غوغل» أن يتبعني بواسطتها. أستخدم أدوات كثيرة للصد في محرك البحث الذي استعمله بهدف منع «غوغل» من ملاحظتي بدقة⁽⁷⁶⁾، لكنني أعلم أن «غوغل» يعمل على تقنيات تستطيع احتواء إجراءاتي الأمنية كافة.

لا أستخدم بريد «جي ميل» (G-mail) الإلكتروني، بل أستفيد بدلاً من ذلك من «مقدم خدمة الإنترنت» (اختصاراً: «آي بي إس» IPS) المحلي، وأخزن بريدي الإلكتروني على كومبيوتري. مع ذلك، يملك «غوغل» ثلث رسائلي⁽⁷⁷⁾؛ لأن كثيرين ممن أتراسل معهم يستخدمون «جي ميل». ولا يقتصر الأمر على العناوين في موقع «جي ميل. كوم»؛ لأن «غوغل» يستضيف مجموعة كبيرة من المؤسسات التي تقدم خدمات البريد الإلكتروني، على الرغم من أن تلك المؤسسات تحتفظ باسم نطاق علوي «دومين نيم» (Domain Name) خاص بها، فلا يظهر مصطلح «جي ميل. كوم» في نهاية عناوينها. ثمة أمثلة أخرى كثيرة. تملك شركة «آبل» (Apple) قاعدة بيانات عن كلمات المرور على موجات الـ «واي - فاي» (Wi-Fi)، من بينها الـ «واي - فاي» في منزلي؛ تجمعها من الناس كلما أجروا عملية صنع ملفات احتياطية

«باك آب» (Back Up) هو اتفهم. وتملك شركات كثيرة معلومات اتصالية عني؛ لأن أصدقائي وزملائي يحفظون بملفات احتياطية عن دفاتر عناوينهم، في مخازن رقمية ضخمة تسمى «سحابة معلومات»، أو «كلاود» (Cloud). إذا نشرت أختي ملفاً يحتوي تركيبتها الجينية، يصبح نصف تركيبي الجيني معروفاً ومشاعاً عاماً أيضاً.

أحياناً، هناك معلومات نتقصد مشاركتها مع نفر قليل، لكنها تغدو معلومات متاحة للرقابة عالمياً. إذ تلتقط إحداهن صورة مع صديق لها في حفلة وتضعها على «فيسبوك»، كي تراها صديقاتها. لكن تلك الصورة تصبح متاحة للعموم ما لم تتقصد عكس ذلك. وبالطبع، يبقى العثور على تلك الصور أمراً صعباً، إلى أن يتعرف نظام مؤتمت إلى الوجوه، ويضع تذيلاً خاصاً عليها، ثم يعمل محرك للبحث على فهرستها. حينها يسهل الوصول إلى تلك الصورة بواسطة محرك بحث للصور. أظهر باستمرار على كاميرات مخصصة لرقابة آخرين. ففي مدن كلندن وشيكاغو ومكسيكو سيتي وبيجينغ، ثبتت قوات الشرطة كاميرات رقابة في الأماكن كافة⁽⁷⁸⁾. وفي مدن أخرى كنيويورك، تعود ملكية كاميرات مماثلة إلى القطاع الخاص. وقد ظهر لنا الفارق بين الأمرين في حادثين إرهابيين. في لندن، جرى التعرف إلى مفجّري مترو الأنفاق بواسطة كاميرات الحكومة، أما في ماراثون «بوسطن»، فقد تولّت المهمة عينها كاميرات ملحقة بشركات خاصة.

من شبه المؤكد أن تلك معلومات رقمية⁽⁷⁹⁾، وغالباً ما تخزن في الكاميرا على دائرة فلمية مغلقة تحو المعلومات القديمة مع تسجيلها معلومات جديدة. لكن يتزايد الميل إلى وضع فيديو الرقابة ذاك على شبكة الإنترنت، ما يؤدي إلى تخزينه إلى ما لا نهاية - فيغدو قسم كبير منه متاحاً للعموم بواسطة محركات البحث.

ما لم نتخذ خطوات لمنع ذلك، سوف تندني إلى حد أبعد إمكانيّة تجنبنا الظهور على كاميرات الآخرين مع زيادة انتشار كاميرات تسجيل الحياة. فحين يقوم عدد كافٍ من الناس بتصوير ما يشاهدونه بانتظام، سوف تظهر في عدد كافٍ من لقطات

فيديوهاتهم بحيث لا يعود مهمماً ما إذا كنت تحمل كاميرا وتصور حياتك اليومية أم لا. إنه نوع من مناعة القطيع، لكن بطريقة معاكسة.

الرقابة الشاملة

ابتكر الفيلسوف جيرمي بنتام تصميمه المعروف باسم «الرقابة الشاملة» («بان أوبتيكون»/ Panopticon^(*)) في أواخر القرن الثامن عشر كطريقة أرخص لبناء السجون. وتتمثل فكرته في تشييد سجن فيه كل نزيل تحت الرقابة كل الوقت، من دون أن يدري. ولا يملك النزيل خياراً سوى افتراض أنه مراقب دائماً، ولذلك يذعن ويتكيف مع الوضع. استُخدمت تلك الفكرة مجازاً لجمع المعلومات الشخصية عن الجموع⁽⁸¹⁾، سواء أكانوا على الإنترنت أم خارجها⁽⁸²⁾.

على الإنترنت، الرقابة شاملة. كلنا قيد المراقبة⁽⁸³⁾ كل الوقت، وتلك المعلومات تخزن إلى الأبد. ذلك ما يبدو عليه حال الرقابة في عصر المعلوماتية، وهي أكثر فعالية من أشد أحلام بنتام جموحاً.

(*) يتكوّن المصطلح من مقطعي "بان" (pan) بمعنى «شامل»، و«أوبتيكون» (opticon) بمعنى «إبصار»، والمعنى هو سجن يمكن رؤية أو مراقبة كل من فيه على مدار الساعة.

3

تحليل بياناتنا

في العام 2012، نشرت صحيفة نيويورك تايمس مقالاً يبيّن أن الشركات تحلّل معلوماتنا، خدمة لغايات إعلانية. وكشف المقال أن شركة «تارغِت» (Target) (*) تستند إلى تحليل ميول الشراء لدى زبائنهم لمعرفة إن كُنَّ حوامل أم لا، وتستخدم تلك المعلومة بأن ترسل لهن إعلانات وكوبونات عن سلع مخصّصة للمواليد. شمل المقال قصة تفصيليّة عن رجل من مدينة «مينابوليس» الأميركيّة تقدّم بشكوى بصدّد قيام «تارغِت» بإرسال كوبونات تتعلق بسلع المواليد إلى ابنته المراهقة، ثم اكتشف لاحقاً أنّ «تارغِت» كانت على حق⁽¹⁾!

تسمّى ممارسة جمع البيانات وتخزينها بأنواعها كافة⁽²⁾ «البيانات الضخمة» (Big Data)، ويسمى علم هندسة استخراج معلومات مفيدة منها «التنقيب في البيانات» (Data Mining). وتنقّب شركات كـ«تارغِت» في البيانات لتركيز حملاتها الإعلانية. الرئيس باراك أوباما اعتمد على أسلوب التنقيب الكثيف في البيانات أثناء حملتيه الرئاسيتين في 2008 و2012، للهدف نفسه⁽³⁾. وتنقّب الشركات في المعلومات التي تحصل عليها من سيّاراتكم، كي تصنع سيارات أفضل؛ وتنقّب البلديات في البيانات التي تحصل عليها من المجسّات المنشورة في الطرقات كي تفهم

(*) تعتبر شركة «تارغِت» ثاني أكبر شركات أميركا للبيع بالتجزئة، بعد شركة «وال مارت» (Walmart) الشهيرة.

ظروف قيادة المركبات. ويجري التنقيب في المعلومات عن تراكيبنا الجينية خدمة لأنواع البحوث الطبية كافة. وتنقّب شركات كـ «فيسبوك» و«تويتر» في بياناتنا لغايات إعلانية، كما سمحت للعلماء بالتنقيب في تلك البيانات خدمة للبحوث الاجتماعية⁽⁴⁾.

تمثّل تلك الأمور كلها الاستخدامات الجانبية للبيانات. ويقصد من ذلك القول إنها لا تمثّل السبب الأصلي لجمع المعلومات. الحال أن الوعد الأساسي لـ «البيانات الضخمة» هو: «خزّن كل ما تستطيع الوصول إليه، وسيكون مستطاعاً ذات يوم التوصل إلى شيء ما مفيد منها».

تملك «البيانات الضخمة» قيمة مشتقة جزئياً من الاستنتاجات التي يمكن أن تستخلص منها. بعض تلك الاستنتاجات واضح تماماً. إذا امتلكت معلومات مكانيّة عن تحركات شخص ما خلال سنة بأكملها، بإمكانك أن تستنتج المطاعم المفضّلة لديه. إذا حزت قائمة بالأشخاص الذين يتحدث إليهم ويراسلهم إلكترونياً، فبإمكانك أن تستخلص من هم أصدقائه. وإذا كانت لديك قائمة بمواقع الإنترنت التي يتردّد عليها - أو ربما قائمة الكتب التي اشتراها - فيمكنك أن تستنتج اهتماماته.

بعض الاستنتاجات أكثر فطنة. قائمة مشتريات البقالة لشخص ما قد توحى بإثنيها، أو عمرها وجنوسها، وربما دينها، أو تاريخها الطبي وعاداتها في تناول المشروبات الروحية. ويتحرّى المسوّقون باستمرار عن أنماط يمكن أن تنبئ بأن شخصاً ما على وشك الإنفاق ببذخ، كإقامة حفل زواج، والذهاب في عطلة، وشراء منزل، وقدوم مولود، وما إلى ذلك. في بلدان عدّة، تستخدم الشرطة تلك البيانات كأدلة إثبات، إما سراً أو أمام المحاكم. ويمكن لحساب على «فيسبوك» أن يشي بمعلومات عن الأصل العرقي لمستخدمه وشخصيته⁽⁵⁾، خياراته الجنسيّة، أيديولوجيته السياسيّة، وضعيّة علاقاته الشخصيّة، واستخدامه مواد مكيفّة؛

ويجري ذلك كله استناداً إلى مجرد التعرّف إلى أنماط استعماله لزر «لايك» في «فيسبوك». يستطيع «فيسبوك» أن يعرف خطوبتك قبل إعلانها⁽⁶⁾، أو كونك مثلي الجنس قبل أن تقرّر إشهار ذلك علانية⁽⁷⁾ - بل إن التدوينات عليه ربما تكشف تلك الأمور للآخرين من دون إذنك ولا حتى معرفتك⁽⁸⁾. ووفقاً للبلد الذي تقطنه، من المحتمل أن تشكل تلك الأمور إحراجاً كبيراً، أو ربما تتسبّب في مقتل⁽⁹⁾.

هناك عدد كبير من الأخطاء في تلك الاستدلالات، وكثيرون منا اختبروا وصول إعلانات بواسطة الإنترنت إليهم، ولم تكن تعنيهم فعلياً إلا بأقل من القليل. في المقابل، عندما تصيب تلك الإعلانات هدفها⁽¹⁰⁾ فإنها تثير خضّة مرعبة، وغالباً ما تكون مموجة. هناك فارق كبير بين الحالين. أنت ترى أحياناً إعلانات عن تحميل طيبة لعلاج البواسير، أو إعلانات على التلفزيون عن خدمات تساعدك في التعرّف إلى فتاة بغرض الصداقة، وحينها، تكون على علم بأنها إعلانات عمومية وموجهة إلى الجمهور بمجمله. ثمة فارق كبير بين تلك الحال، وبين أن تصلنا إعلانات تكون موجهة إلينا تحديداً⁽¹¹⁾، ومستندة إلى تدويناتنا على الإنترنت أو مواقع زرناها على الشبكة، فتبدو كأنها نوع من الاجتياح. إذ يتولّد عن ذلك توتر مثير للاهتمام: المعلومات التي رغبتنا في مشاركتها مع الآخرين تقود إلى استنتاجات لا نرغب في التشارك بها أبداً. يرحب عديدون بأن يقدموا لشركة «تارغيت» معلومات عن أنماط مشترياتهم للحصول على تخفيضات وإشعارات بخصوص منتجات جديدة ربما يرغبون في شرائها؛ لكن معظمنا ربما لا يرغب في أن يخبر «تارغيت» بحدوث حال حمل. وكذلك فإننا لا نستطيع عمليات السرقة والسطو على المعلومات التي تضرب بصورة محتمّة قواعد المعلومات المتصلة بـ «البيانات الضخمة».

حين نفكر بأن الكمبيوترات تستخدم كل معلوماتنا في صنع استدلالات واستنتاجات عنا، نصل إلى طريقة إنسانية تماماً في التفكير بصدد تلك الآلات. نحن نفكر في ما يمكن أن نستنتجه من المعلومات، ثم نسقط ذلك على الكمبيوترات. ليست تلك بطريقة صائبة للتفكير بشأن الحواسيب. ثمة فوارق في القوى

والمحدّدات ونقاط الضعف، بين البشر والكومبيوترات. إذ لا يستطيع الكومبيوتر ممارسة التفكير المجرّد مثلما يفعل معظم البشر، لكن الآلات تستطيع التعامل مع كمّيات كبيرة من المعلومات، وبطريقة تتزايد سرعتها باستمرار. (من المستطاع التفكير بأن ذلك يعني أن الكومبيوتر متفوّق في التعامل مع «البيانات الوصفية»، أكثر من التعامل مع تفاصيل المكالمات والحوارات). وتتزايد قوّة الكومبيوترات باطراد، إذ ما زالت قوّتها تتضاعف كل 18 شهراً، فيما يظل حجم دماغ الجنس الإنساني ثابتاً. وحاضراً، تتفوّق الحواسيب على البشر في التعامل مع المعلومات الكميّة، بل إن قوّتها تتحسّن على نحو مطّرد.

في الوضع الراهن، يمثّل التنقيب في المعلومات تقنية «ساختنة»⁽¹²⁾، بمعنى أنها موضع اهتمام فائق، إضافة لكونها محاطة بكثير من الادّعاءات والهالات والانتهازية. ليس من الواضح كلياً أنواع البحوث الممكنة في ذلك الحقل، ولا القوى الكامنة فعلياً فيه. في المقابل، من البيّن أن تقنية التنقيب في البيانات تتزايد قوّتها، وتعطي المراقبين قدرة متعاظمة على التوصل إلى استنتاجات مذهلة من المجموعات المتراكمة من «البيانات الضخمة».

الرقابة في أزمنة مضت

ثمة شيء جديد يمكنك فعله بتطبيق تقنية التنقيب في البيانات على الرقابة العامة، يتمثّل في الرجوع إلى الماضي⁽¹³⁾. إذ تمحورت الرقابة التقليدية على الحاضر والمستقبل: «راقب ذلك الشخص، وتعرّف إلى خطوته التالية». ولكن، عندما تحوز قاعدة معلومات فيها معلومات متراكمة زمنياً عن كل شخص، حينها تستطيع فعل شيء جديد: «دقّق في تلك «المعلومات المكانيّة» عن ذلك الشخص، وتعرّف إلى الأمكنة التي يوجد فيها؛ أو «استمع إلى مكالماته أثناء الأسبوع الماضي».

في الماضي، كانت بعض تلك الأشياء ممكنة أيضاً. وتاريخياً، دأبت الحكومات على جمع كل أنواع المعلومات. ففي الحقبة المكارثية^(*) على سبيل المثال، استخدمت الحكومة سجلات الأحزاب السياسية، والاشتراكات في المجلات، وشهادات من الأصدقاء والعائلة والجيران والزملاء؛ بهدف جمع المعلومات عن الناس. والفارق بين ذلك الماضي وما يحدث حاضراً يتمثل في أن القدرة على الرقابة باتت تشبه صنع آلة الرجوع إلى الماضي: إذ صارت البيانات أكثر دقة واكتمالاً، وتدنت تكلفة الحصول عليها، وتطوّرت التكنولوجيات بما يعطي القدرة على الإتيان بتحليل تاريخي متطور. مثلاً، في السنوات القليلة الماضية، أقرّت بنوك «كريدي سويس» و«ستاندرد شارتز» و«بي آن بي باريا»، بأنها اخترقت قوانين حظر نقل الأموال إلى مجموعات قيد المراقبة. وغيّرت المؤسسات تلك البيانات للتملّص من ترصد الجداول الحوارزمية ورقابتها لـ «فلاتر أوفاك»، وهي اختصار لـ «مكتب رصد الأصول المالية الأجنبية» التابع لـ «الحزنة العامة» الأميركية. واستلزم التعرّف إلى ذلك النوع من التملّص الجرمي⁽¹⁴⁾ إجراء تحليل تاريخي مكثّف لأزمة المعاملات المالية والاتصالات بين الموظفين.

وعلى نحو مشابه، من المستطاع استخدام أدوات تحليلية مبتكرة، للتنقيب في معلومات قديمة. لنفكر في البيانات عن التركيبة الجينية للأفراد. حاضراً، ليس هناك الكثير مما يمكن استخلاصه من تحليل التركيبة الجينية للفرد، لكن بعد عشر سنوات - من يعرف كيف تكون الأمور حينها؟ لقد رأينا شيئاً مشابهاً يحصل في اختبارات المنشطات في سباقات «تور دي فرانس» للدراجات الهوائية. وعندما جرى تحليل عينات دم أخذت قبل سنوات من درّاجين⁽¹⁵⁾، بواسطة أساليب أكثر جدّة؛ تفجّرت فضيحة انتشار المنشطات في تلك المنافسة.

(*) إشارة إلى فترة في مطالع الخمسينيات من القرن العشرين، استطاع فيها السيناتور الجمهوري جو مكارثي تحريض الحكومة الأميركية على ممارسة رقابة واسعة تحت شعار محاربة الشيوعية.

تخزن «وكالة الأمن القومي» سيولاً من المعلومات المتراكمة من أزمان ماضية، وهو أمر سأتحدث عنه بتفصيل أكبر في الفصل الخامس. نعرف أنه في العام 2008، كان لدى الوكالة قاعدة معلومات تسمى «إكس كي سكور» (XKEYSCORE)⁽¹⁶⁾، تحتفظ روتينياً بتسجيلات صوتية للمكالمات لمدة ثلاثة أيام، لكنها تخزن الـ «ميتاداتا» عنها لمدة شهر كامل. وفي قاعدة بيانات أخرى لـ «وكالة الأمن القومي» تحمل اسم «مارينا» (MARINA)⁽¹⁷⁾ تجمع معلومات عن عمليات تصفّح الجمهورر للـ «ويب» لمدة سنة. وفي قاعدة بيانات أخرى اسمها «ميستيك» (MYSTIC)⁽¹⁸⁾، احتفظت الوكالة بتسجيلات المكالمات الهاتفية كافة، التي تمر من تحت مياه جزيرة «برمودا» وهي محطة رئيسة للكوابل البحرية للاتصالات بواسطة الهواتف الأرضية، التي تصل بين أميركا ومعظم الدول الغريبة. وتحتفظ الوكالة بـ «ميتاداتا» الهواتف لخمس سنوات⁽¹⁹⁾.

تنطبق حدود تلك المدد الزمنية للتخزين على المعلومات كافة. وفي حال تلمس أحد عملاء الوكالة شيئاً ما في قواعد المعلومات، تحتفظ الوكالة بذلك النوع من البيانات لمدة أطول. إذا كانت المعلومات عنك متأتية من بحث استقصائي في تلك القواعد للبيانات، يجري الاحتفاظ بها إلى الأبد. إذا استخدمت التشفير، يجري الاحتفاظ بمعلوماتك إلى الأبد⁽²⁰⁾.

تعلّق مدة تخزين المعلومات لدى «وكالة الأمن القومي» بالقدرات التقنية أكثر من احترامها الخصوصية. نعرف أن الوكالة احتاجت لزيادة قدراتها على تخزين كل المعلومات التي جمعتها عن مواقع الهواتف الخلوية⁽²¹⁾. ومع التدني المستمر في تكلفة تخزين البيانات، يمكن التفكير بأن مزيداً منها سيُحتفظ به لمدد أطول. عند تلك النقطة⁽²²⁾، تظهر الفكرة من «مركز يوتاه للمعلومات» الذي أنشأته «وكالة الأمن القومي».

تحتفظ وكالة الـ «إف بي آي» بالمعلومات أيضاً⁽²³⁾. وفي غمار تحقيق قانوني جرى في 2013، حصلت الـ «إف بي آي» على نسخة عن البيانات الموجودة كافة في موقع يسمّى «فريدم هوستنج» (Freedom Hosting)، بما في ذلك رسائل البريد الإلكتروني المخزنة عليه. كانت معظم البيانات غير متعلّقة بالتحقيق مباشرة، لكن الـ «إف بي آي» احتفظت بنسخة عن الموقع برمّته؛ ومنذها، باتت تدخل عليه تكراراً أثناء تحقيقات لا تتعلق به. وتحتفظ ولاية نيويورك بمعلومات عن القارات الضوئية للوحدات المركبات، لخمس سنوات على الأقل وربما إلى ما لا نهاية⁽²⁴⁾.

من المستطاع مبدئياً الاحتفاظ بالمعلومات كافة كسجلات التواريخ في «فيسبوك»، والتغريدات، وصور لوحات المركبات، إلى ما لا نهاية، أو إلى أن يتقرّر حذفها من قبل الشركة أو الوكالة الحكومة المعنية. في 2010، كانت شركات الخلوي تحتفظ بالرسائل النصيّة لما يتراوح بين 90 يوماً و18 شهراً. وتفوّقت عليهم جميعاً شركة «إيه تي أند تي» (AT&T)⁽²⁵⁾، بأن توصّلت إلى الاحتفاظ بتلك الرسائل لسبع سنوات.

وضع خرائط العلاقات

تفتح المعلومات المستقاة من الرقابة العامة الباب أمام إمكانية رسم خرائط للعلاقات الشخصية بين الأفراد. في 2013، عندما عرف الناس للمرة الأولى أن «وكالة الأمن القومي» دأبت على جمع «بيانات وصفية» عن مكالمات الأميركيين كلهم، ثار ضجيج كبير حول ما سُمّي «البحوث النّطّاطة» وما تعنيه فعلياً. إذ إنّها تمثّل نوعاً جديداً من البحوث كانت ممكنة نظرياً قبل عصر الكمبيوتر، لكنها لم تغدُ عملية بصورة فعلية إلا بعد الرقابة الرقمية العامة. تحيّل مثلاً أن «وكالة الأمن القومي» وجّهت اهتمامها صوب فتاة ما تدعى أليس. سوف تجمع الوكالة معلومات عن تلك الفتاة، ثم معلومات عن كل الأشخاص الذين اتّصلت بهم، ثم معلومات عن الأشخاص الذين اتّصلوا بأولئك الأشخاص، ثم معلومات عن الأشخاص

الذين اتصل الأخيرون بهم. بذا، تكون الوكالة على بُعد ثلاث «قفزات» من أليس، وهو الحد الأقصى الذي تعمل الوكالة في نطاقه.

يتمثل القصد من «البحوث النطّاطة» في رسم خريطة عن العلاقات والتحري عن وجود تأمر ما. وكي تغدو تلك المعلومات مجدية⁽²⁶⁾، يجب استبعاد غالبية ساحقة من أشخاص أبرياء في تلك الشبكة المُتَصِّدَة، وأرقام الهواتف المألوف استخدامها من قِبَل أولئك الأبرياء⁽²⁷⁾: شركات خدمة البريد الصوتي، ومطاعم الـ «بيتزا»، وشركات سيارات الأجرة، وهكذا دواليك.

تشير وثائق «وكالة الأمن القومي»⁽²⁸⁾ إلى أنها لاحقت 117675 «هدفاً ناشطاً للرقابة» في يوم واحد في 2013. وإذا استخدمنا التقديرات الأشد تحفظاً عن عدد الأشخاص الذين يتحدث إليهم المرء ومدى تشابكهم مع آخرين، سوف يتجاوز العدد الكلي للأشخاص الموضوعين قيد الرقابة في ذلك اليوم بسهولة ما يربو عن 20 مليون شخص⁽²⁹⁾. يعطي ذلك مثلاً كلاسيكياً عن مسألة «الحلقات الست» في العلاقات بين الناس، بمعنى أن هناك عموماً ست دوائر (أو ست «قفزات»، وفق تعابير «البحوث النطّاطة») تفصل بين كل شخص وآخر في الولايات المتحدة. في العام 2014، طلب الرئيس باراك أوباما⁽³⁰⁾ من «وكالة الأمن القومي» أن تقتصر «البحوث النطّاطة» على «قفزتين» في تحليل «البيانات الوصفية» لأرقام الهواتف الموضوعية تحت رقابة برنامج ما للوكالة، لكن الرئيس لم يضع قيوداً على عدد تلك «القفزات» في الأنواع الأخرى من المعلومات التي تجمعها الوكالة.

تشكّل «البيانات الوصفية» المستقاة من مصادر متنوعة أداة قويّة في رسم خرائط العلاقات الشخصية. إذ تستخدم غالبيتنا الإنترنت في التواصل الاجتماعي بواسطة الـ «سوشال ميديا»، وتظهر علاقاتنا الشخصية فيها. كذلك فإنّه بالضبط ما تشارك فيه معاً «وكالة الأمن القومي» وشركة «فيسبوك»⁽³¹⁾، وهو السبب في أن الأخيرة

تقترح عليك ببرود أسماء أشخاص ربما تكون تعرفت إليهم، لكنك لم تضعهم في قائمة الأصدقاء في حسابك على «فيسبوك».

يتمثل أحد أكثر مناحي برامج «فيسبوك»⁽³²⁾ الإعلانية نجاحاً في عدم اقتصارها على إبراز الإعلانات الترويجية على شاشات كل مَنْ ضغط على زر «أعجبني» عند مشاهدة سلعة أو صفحة، بل أيضاً إلى أصدقائهم ثم أصدقاء أصدقائهم أيضاً.

التحري عنا بأفعالنا

بعد أن تتجمع المعلومات عن كل شخص، يصبح ممكناً العثور على كل فرد تتبع سلوكياته. ربما رغبت في معرفة كل من يتردد على مقصف مخصص للمثليين جنسياً، أو يطالع مواضيع معينة، أو يمتلك أفكاراً سياسية محددة. تتولى الشركات معرفة تلك الأمور بصورة منتظمة بواسطة استعمال معلومات الرقابة الرقمية العامة، كي تعثر على مستهلكين محتملين لهم تفضيلات معينة، أو إيجاد أشخاص ترغب في توظيفهم بواسطة البحث عن نشر أشياء عن موضوعات بعينها.

من المستطاع التفتيش عن أشياء غير الأسماء والمعرفات الشخصية الأخرى كرقم الهوية والهاتف وغيرهما. مثلاً، يفتش «غوغل» كل رسائلك في «جي ميل»⁽³³⁾، ثم يستخدم الكلمات المفتاحية التي عثر عليها، كي يتوسّع في فهم شخصيتك، وذلك لغايات تتعلق بالإعلانات. تفعل «وكالة الأمن القومي» أمراً مُشابهاً⁽³⁴⁾، لكنها تسميه «بحوث الـ «حَوْل»». وبصورة أساسية، يعمل ذلك النوع من البحوث عبر التفتيش في محتوى الاتصالات لشخص ما، بحثاً عن كلمات أو أسماء معينة - أو ربما عبارة بعينها. فإذا، إضافة إلى التفتيش في البيانات المتعلقة بآليس والأشخاص الذين تشملهم «قفزتان» أو ثلاث «قفزات» حولها، تستطيع الوكالة أن تفتش معلومات الأشخاص كافة - بمعنى التفتيش في قواعد بيانات الاتصالات كافة - بحثاً عن اسمها. وإذا لم تكن الوكالة على معرفة باسم آليس، لكنها تعرف مشروعاً أو مكاناً أو اسماً حركياً يستخدمه أحدهم في الإشارة إلى آليس؛ تستطيع إجراء بحوث انطلاقاً

من تلك المعلومات. ومثلاً، تستهدف «وكالة الأمن القومي» الأشخاص الذين يبحثون عن أدوات رقمية تتعلق بالخصوصية على الإنترنت أو بإخفاء الشخصية عليها⁽³⁵⁾.

لا نعرف التفاصيل، لكن «وكالة الأمن القومي» تعتمد إلى ربط سلاسل من «البحوث النطاطة»⁽³⁶⁾، انطلاقاً من أي علاقة تقع تحت يدها؛ ولا يقتصر الأمر على الاتصالات الهاتفية. إذ يحتمل أن يشمل ذلك الربط وجودك في المكان عينه مع شخص تحت الرقابة⁽³⁷⁾، أو وجود أشخاص مشتركين بينك وبينه في الاتصالات، وما إلى ذلك. بات ممكناً إجراء تلك الأنواع من البحوث بفضل القدرة على الوصول إلى بيانات الناس كلها.

من المستطاع استخدام الرقابة العامة للعثور على أشخاص معينين. إذا علمت أن شخصاً ما كان في مطعم معين في ليلة بعينها، وقصد محطة مترو ذات ظهيرة بعد ثلاثة أيام، واقترب من محطة كهربائية في الصباح التالي؛ تستطيع إجراء تحقيق في قواعد البيانات عن مواقع الهواتف للناس كافة، فيظهر فوراً الأشخاص الذين تنطبق عليهم المواصفات السابقة.

من المستطاع أيضاً التفتيش عن السلوك الخارج عن المؤلف. في ما يلي أربعة أمثلة عن الطرق التي تستعملها «وكالة الأمن القومي» في تحليل معلومات الخلوي.

(1) تستعمل الوكالة «المعلومات المكانية» للخلوي⁽³⁸⁾؛ كي تتبع الأفراد الذين تتقاطع مواقع أمكنتهم. لنفترض أن الوكالة مهتمة بآليس. إذا تبين أن شخصاً اسمه بوب كان في المطعم الذي قصده آليس ذات مساء، وكذلك في المقهى الذي تناولت فيه القهوة صباحاً بعد أسبوع، وفي نفس المطار الذي توجهت إليه آليس بعد شهر؛ سوف يشير النظام المعلوماتي للوكالة إلى بوب بوصفه مشاركاً محتملاً مع آليس، حتى لو لم يتواصل الشخصان إلكترونياً.

(2) تتعقب الوكالة مواقع أجهزة الخلوي التي يحملها جواسيس أميركا في الخارج⁽³⁹⁾، ثم تحدد إذا كان ثمة خلوي آخر يتتبع الهاتف المحمول لأحد جواسيس أميركا. وأساساً، تتعقب الوكالة إذا كان ثمة من يلاحق أولئك الجواسيس.

(3) تملك الوكالة برنامجاً لتصيد «البيانات الوصفية» عن الهواتف⁽⁴⁰⁾، يستطيع ملاحظة الخلويات التي استُعملت لفترة وجيزة ثم أقفلت ولم يُعاود أحد تشغيلها لاحقاً أبداً. وتستخدم الوكالة المعلومات عن أنماط استخدام الخلويات كي تربط بينها. وتوظف تلك التقنية لمعرفة الهواتف «المحروقة»، بمعنى أنها استُخدمت من قبل أشخاص يسعون لتجنب الرقابة.

(4) تجمع الوكالة معلومات عمّن أطفأوا هواتفهم، إضافة إلى المدة التي تبقى فيها مطفأة⁽⁴¹⁾. ثم تجمع بيانات عن الأمكنة التي يعاود فيها أولئك الأشخاص تشغيل هواتفهم فيها. وكذلك تجمع معلومات عن أشخاص آخرين أغلقوا هواتفهم في أمكنة قريبة من المجموعة الأولى. بقول أوضح، تسعى الوكالة إلى رصد الاجتماعات السرية.

سبق أن ناقشتُ الطريقة التي استخدمت فيها الحكومة الأوكرائية «المعلومات المكانية» عن الخلويات، بهدف التعرف إلى كل من شارك في تظاهرات معارضة لها، وكذلك الأمر بالنسبة لاستعمال شرطة ولاية «ميشغن» لـ «البيانات المكانية» عن الخلويات للتعرف إلى من كانوا قرب مكان لتجمع نقابي احتجاجي مزع. وتستعمل الـ «إف بي آي» تلك البيانات لملاحقة خلويات يستعملها أشخاص تحت الرقابة، لكن لا تربطها بهم علاقات أخرى⁽⁴²⁾.

تفعل الشركات أشياء مشابهة أيضاً. ثمة تقنية تسمى «التطويق الجغرافي»، يستعملها المسوّقون للتعرف إلى الأشخاص عندما يكونون قرب مراكز تجارية

معينة، كي تُرسل لهم موادَّ إعلانية. تقدّم إحدى شركات «التطويق الجغرافي»⁽⁴³⁾، اسمها «بلايس كاست» (Place cast)، إعلانات تجارية مستندة إلى المواقع الجغرافية، وترسلها إلى عشرة ملايين خلوي في الولايات المتحدة والمملكة المتحدة، كي تصلهم عندما يكونون قرب سلاسل المخازن الكبرى كـ «ستارباكس» (Starbucks) و«كاي مارت» (K Mart) و«ساب واي» (Subway). تفعل شركة «مايكروسوفت» الأمر نفسه مع الأشخاص الذين يمرون على مسافة عشرة كيلومترات من مخازنها⁽⁴⁴⁾؛ وهي تتعامل مع شركة تعمل في «التطويق الجغرافي» اسمها «ناينث ديسيميل» (NinthDecimal). وتستعمل شركة «سينس نتوركس» البيانات المكانية للخلوي كي تصنع ملفات «بروفایل» عن الأفراد⁽⁴⁵⁾.

تنسيق المجموعات المتنوعة من البيانات

تعدُّ «فيجيلنت سوليوشنز» (Vigilant Solutions) من الشركات التي تجمع بيانات عن لوحات المركبات من الكاميرات⁽⁴⁶⁾. وتملك الشركة خططاً لتدعيم نظامها المعلوماتي بجداول خوارزمية أخرى تفيد في التعرف إلى أرقام السيارات، ونُظّم التعرف إلى الوجوه، ومعلومات من قواعد أخرى للبيانات. والنتيجة المتوقعة هي منصة رقابة أشد صرامة ودقة من مجرد قاعدة للبيانات فيها صور للوحات المركبات، بغض عن النظر عن الاتساع الذي تصل إليه تلك المنصة.

غالباً ما يضع الإعلام وقصصه الإخبارية الرقابة العامة ضمن إطار جمع المعلومات والبيانات؛ ولكن تفوته حكاية الربط والتنسيق بين المعلومات، بمعنى ربط الهويات⁽⁴⁷⁾ الموجودة في مجموعات متباينة من قواعد البيانات؛ بهدف التوصل إلى استنتاجات واستدلالات من البيانات المجمعة. لا يتعلق الأمر بمجرد القول إن طائرات «درون» أرخص ثمناً ستصبح أمراً شائعاً تماماً، فيها كاميراتها ستكون أشد قوة. تتمثل المسألة في أن الـ «درون» مع برنامج رقمي للتعرف إلى الوجوه سيتيح للنظام التعرف إلى الناس بطريقة مؤتمتة، إضافة إلى وجود قواعد بيانات ضخمة

للصور المذيلة بتعريفات عمن فيها- وهي مستقاة من رُخص القيادة وصفحات «فيسبوك» والصحف اليومية والكتب السنوية للمدارس الثانوية- وكلها مصادر ترفد ذلك البرنامج بصور مرجعية للأفراد. وكذلك تتعلق المسألة بالربط والتنسيق بين مخرجات ذلك البرنامج للتعرف، مع قواعد بيانات متنوعة أخرى؛ ويُضاف إليها القدرة على تخزين كل تلك المعلومات إلى ما لا نهاية. تتأتى الرقابة الشاملة من جمع سيول المعلومات والبيانات الآتية من مصادر مختلفة، وربطها معاً في كل متكامل.

عندما أكون في لندن، أستخدم بطاقة من شركة «أويستر»⁽⁴⁸⁾ [تتميز بأن بياناتها لا تصل إلى الإنترنت] لدفع بدل النقل في المواصلات العامة. بذلت قصارى جهدي وعناشي كي أبقى على دفع بدل النقل نقداً، ودون التعريف إلى الهوية. وعلى الرغم من ذلك، إذا جرت مقارنة استعمال تلك البطاقة مع قوائم زوار لندن وتواريجها، سواء أكانت تلك القائمة من صنع خطوط الطيران، شركات البطاقات الائتمانية، شركات الخلوي، أم «مقدمي خدمات الإنترنت»؛ فأنا أراهن على أنني الشخص الوحيد الذي سوف تتقاطع عنده تلك المعلومات بتكامل تام. لذا، فإن تحركاتي «الخفية الاسم» في مترو أنفاق لندن، لا تحقق ذلك الهدف أبداً.

كشف سنودن مشروعاً مثيراً للاهتمام تنهض به مؤسسة «سيسك» (CSEC)، وهي اختصار لاسم «مؤسسة أمن الاتصالات في كندا» (Communications Security Establishment Canada)، وهي نظيرة «وكالة الأمن القومي» في ذلك البلد. ويرهن المشروع أهمية الربط والتنسيق بين مسارات مختلفة من معلومات الرقابة للعثور على أشخاص يتقصّدون التملّص منها⁽⁴⁹⁾.

ثمة باحث في «سيسك» تحمل وظيفته لقباً جذاباً هو «مطوّر مهارات الجاسوسية»، انطلق مما يساوي معلومات لمدة أسبوعين مُجمّعت من الإنترنت، ما يعني أساساً أنه عمل على قوائم تعرّف إلى أرقام الهوية للذين دخلوا إلى مواقع مختلفة

على الإنترنت. وكان لديه أيضاً قاعدة بيانات عن المواقع الجغرافية لأرقام التعريف عن المستخدمين للشبكات اللاسلكية للإنترنت. وبمقارنة مجموعتي المعلومات، استطاع ذلك الباحث التوصل إلى ربط أرقام هويات من دخلوا إلى الإنترنت بواسطة شبكات لاسلكية، مع مواقعها الجغرافية. كانت الفكرة من البحث هي العثور على أشخاص. إذا كان لديك رقم هوية استخدام الإنترنت لشخص قيد الرقابة، تستطيع أن تطلق صافرة إنذار عند دخوله شبكة لاسلكية للإنترنت في مطار أو فندق، وبالتالي معرفة موعد سفره. وكذلك تستطيع أن تتعرف إلى شخص معين بمعرفتك المواقع الجغرافية التي عبرها مع التواريخ والأوقات. مثلاً، لنفترض أنك تبحث عن شخص اتصل بك من دون أن يكشف هويته، من ثلاثة مواقع لهواتف عمومية. أنت تعرف أزمته تلك المكالمات ومواقع التليفونات التي أجريت منها. إذا كان في جيب ذلك الشخص هاتف ذكي، فإن الأخير يتصل بصورة أوتوماتيكية مستمرة مع الشبكات اللاسلكية، ما يمكنك من الربط بين تلك الاتصالات الأوتوماتيكية وبين الأوقات والتواريخ التي لديك، وكذلك مواقع تلك الشبكات. والأرجح أنك ستصل بالنتيجة إلى التعرف إلى شخص بعينه.

توصل بحاثه في «جامعة كارنيجي ميلون» إلى فعل شيء مشابه. إذ وضعوا كاميرا رقابة في مكان عام، والتقطوا صوراً لأشخاص يمرون بها، وتعرفوا إليهم بفضل برامج التعرف إلى الوجوه مع قاعدة بيانات «فيسبوك» عن الصور المذيلة بتعريفات، ثم قارنوا الأسماء مع قواعد أخرى للبيانات. وبالنتيجة توصلوا إلى إبراز معلومات شخصية عن الأفراد الذين يمرون بالكاميرا، في لحظة مرورهم بها فعلياً⁽⁵⁰⁾. ومن المستطاع توفير تلك التقنية لكل شخص، بواسطة استعمال كاميرا ذكية أو ارتداء نظارة «غوغل».

أحياناً، يسهل الربط بين الهويات الموجودة في قواعد بيانات مختلفة؛ فاسمك مربوط مع هاتفك الخليوي، وكذلك الحال بالنسبة لبطاعتك الانتخابية. أحياناً، تكون الأمور أكثر صعوبة. إذ ربما لا يكون اسمك مربوطاً فعلياً بريدك الإلكتروني،

إلا في حال أشار من تراسل معهم إليك بالاسم. هناك شركات كـ «إنشيت سيزتمز» (Initiate Systems)، تباع برامج رقمية تربط بين المعلومات الموجودة في قواعد بيانات مختلفة⁽⁵¹⁾؛ وهي تباع تلك البرامج إلى شركات وحكومات. كذلك تعمل الشركات على الربط بين سلوكك على الإنترنت وبين أفعالك الحقيقية خارج الإنترنت. ومثلاً، يتشارك موقع «فيسبوك» مع سمسرة المعلومات كشركتي «إبسلون» (Epsilon) و«أكسيوم» (Acxiom)، للمقارنة بين بروفائلك الشخصي في «فيسبوك» وبين مشترياتك في المخازن الكبرى⁽⁵²⁾.

عندما تتوصل إلى الربط بين مجموعات مختلفة من المعلومات، يغدو باستطاعتك فعل أشياء عدّة بها. تخيل أنك تريد صنع صورة عن صحة شخص ما، من دون أن تعرف ملفه الطبي. تستطيع بيانات البطاقات الائتمانية وبطاقات الشراء من المخازن الكبرى، أن تعطي معلومات عما يفضلُه من مأكولات وما يتناوله من مشروبات كحولية، وكذلك المطاعم التي يقصدها، وإذا كانت لديه عضوية في مركز للرياضة، وماهية الأشياء التي يشتريها من الصيدليات خارج الوصفات الطبية.

ويكشف هاتفه الخلوي عدد المرات التي يقصد فيها المركز الرياضي، وتقدّم أدوات رقابة الحركة معلومات عن مستوى نشاطه البدني هناك. وتكشف البيانات عن المواقع الشبكية التي يستعملها عن نوع المعلومات الطبية التي يهتم بالتفتيش عنها. بواسطة تلك الطُّرُق، تتمكن شركة كـ «إكزاكت داتا» (Exact Data) من بيع قوائم عن الأشخاص الذين ينخرطون في المواعدة بواسطة الإنترنت⁽⁵³⁾، والمقامرين، وأولئك الذين يعانون أمراضاً كالقلق النفسي والتبول اللاإرادي أو اضطراب القدرة على الانتصاب.

اختراق خفائنا

عندما تننصت منظمة قوية على قسم كبير من بنيتنا الإلكترونية التحتية، مع قدرتها على الربط بين مسارات مختلفة من الرقابة، فإنها تستطيع في الغالب أن تتعرف إلى الأشخاص الذين يسعون إلى الخفاء. في ما يلي 4 قصص تبرهن ذلك الأمر.

- (1) جرى التعرف إلى الـ «هاكرز» العسكريين الصينيين⁽⁵⁴⁾، الذين شاركوا في مجموعة واسعة من الهجمات ضد الحكومة والشركات الأميركية؛ لأنهم دخلوا إلى موقع «فيسبوك» مستخدمين البنية الإلكترونية التحتية نفسها التي استعملوها في تنفيذ هجماتهم.
- (2) أخضع هكتور مونزيجر⁽⁵⁵⁾، أحد قادة حركة الـ «هاكرز» تحمل اسم «لولزسيك» (LulzSec)، للتحقيق لأنه اخترق عدداً من الشبكات التجارية، بعد أن تمكنت الـ «إف بي آي» من التعرف إليه واعتقاله في 2011. وعلى رغم أنه أُركن إلى عادات حسنة في أمن الكمبيوتر كما استخدم هوية مغفلة في الحصول على وصلة لدخول الإنترنت، فإنه انزلق ذات مرة. وإذا لم يستطع تجنب الإشارة إلى نفسه أثناء إحدى المحادثات، استطاع محقق في الـ «إف بي آي» أن يتبعه وصولاً إلى الحصول على فيديو من موقع «يوتيوب» (YouTube)، عن سيارته، ثم عثر على صفحته في موقع «فيسبوك».
- (3) في سياق مشابه، اتخذت باولا بردويل⁽⁵⁶⁾ التي أقامت علاقات جنسية مع مدير الـ «سي آي إيه» الجنرال ديفيد بيترايوس، احتياطات واسعة بهدف إخفاء هويتها. ولم تدخل أبداً على بريدها الإلكتروني الذي لا يحمل هويتها من منزلها. وبدلاً من ذلك، استعملت شبكات في فنادق وأماكن عامة للتراسل مع بيترايوس. وقارنت الـ «سي آي إيه» معلومات التسجيل من فنادق مختلفة، وسرعان ما ظهر اسم مشترك (باولا بردويل) بينها.

(4) هناك «هاكر» سمّي نفسه «ورمر» وكان ناشطاً ضمن مجموعة الـ «هاكرز» المعروفة باسم «أنونيموس» (Anonymous) ⁽⁵⁷⁾، كما كان مطلوباً بسبب اختراقه مواقع أمنية أميركية. واستخدم حساباً غفل الهوية على «تويتر»، لكنه وضع صورة لصدر امرأة التقطها بهاتف «آي فون». وتضمّن ملف الصورة معلومات الـ «جي بي إس» عنها، ما أتاح تحديد أنها التُقطت في منزل في أستراليا. وهناك موقع آخر، أشار إليه «ورمر»، لكنه كان يتضمن اسم هينغينو أو شاوا أيضاً. وتراقب الشرطة صفحة أو شاوا على «فيسبوك» التي تضمّنت معلومة تفيد بأن لديه صديقة أسترالية. وتطابقت صور تلك الصديقة مع الصورة الأولى التي انطلق منها التحقيق. وبذا، استطاعت الشرطة أن تعتقل أو شاوا الذي يحمل اسماً حركياً هو «ورمر».

يكاد إخفاء الهوية أن يكون مستحيلاً على الإنترنت حيال مراقب كلي القدرة. إذا نسيت لمرة تفعيل حماياتك، إذا ضغطت على رابط إلكتروني لا يجدر بك التعامل معه، إذا طبعت شيئاً ما بالخطأ؛ تربط اسمك بشكل دائم مع من قدّم لك خدمة إخفاء الهوية على الإنترنت. إنّ المستوى العملي للاستمرار في الاحتفاظ بالخصوصية وإخفاء الهوية على الإنترنت، في مواجهة تحقيق موجه ومصمّم على الوصول إليك، يفوق مصادر حتى العملاء الحكوميين المدربين جيّداً. وحتى فريق اغتيال إسرائيلي مدرب على مستوى متقدّم، انكشف بسرعة في دبي، استناداً إلى تذييلات كاميرات الرقابة في المدينة ⁽⁵⁸⁾.

ينطبق الأمر عينه على مجموعات كبيرة من البيانات المغفلة الهوية. لربما راودنا الاعتقاد الساذج بأن عددنا كبير إلى حدّ أنّه من المستطاع الاختباء في ذلك البحر من البيانات؛ أو أن معظم معلوماتنا خفية الهوية. كل ذلك ليس صحيحاً. إذ إنّ معظم

تقنيات إخفاء الهوية فاشلة⁽⁵⁹⁾، ومن الممكن إعادة وضع الهوية على البيانات انطلاقاً من معلومات فائقة الضائكة.

في العام 2006، أصدرت شركة «إيه أو إل» (AOL) بيانات عن عمليات التفتيش على الشبكة التي أجراها 657 ألف مستخدم، وبلغ عددها قرابة 20 مليون عملية. قصدت الشركة أن تكون البيانات مفيدة للبحثة، لذا سعت إلى حماية هوية الأشخاص باستبدالها بأرقام. لنقل إنها أعطت الكاتب بروس شنابير رقماً هو 608429. وتفاجأت الشركة عندما تمكّن البحثة من التوصل إلى الأسماء⁽⁶⁰⁾، بواسطة ربط المكونات المختلفة في ملف عمليات التفتيش التي أجراها الأفراد على الإنترنت.

في 2008، نشرت شركة «نتفليكس» (Netflix) عشرة ملايين تقييم للأفلام عبّرت عن آراء نصف مليون مستخدم، لم تكشف عن هوياتهم. جاءت الخطوة ضمن تحدّ أطلقته الشركة للجمهور العام بأن يأتي بنظام لتقييم الأفلام أفضل مما كانت الشركة تستعمله في ذلك الوقت. واستطاع بحثة أن يتعرفوا إلى الهويات المغفلة للمستخدمين⁽⁶¹⁾، بمقارنة التقييمات وتذييلات الوقت مع ما يقابلها في موقع «إنترنت موفي داتا بيز» (Internet Movie Database)، الذي يعدّ أضخم قاعدة بيانات عن أفلام السينما يتفاعل معها جمهور الإنترنت.

ربما بدت تلك الأمثلة كأنها تعبّر عن حالات خاصة، لكن فرص ملاحظة عمليات ربط البيانات تتكرّر بأكثر مما تظن⁽⁶²⁾. إذا استطاع شخص ما النفاذ إلى قاعدة بيانات لأرقام الهواتف لا تحتوي على أسماء، فإنه يستطيع التوصل إلى معرفة أسماء أصحابها بربطها بقاعدة بيانات عن مكالمات تسوّق البضائع وطلبيّاتها. وعلى نحو مشابه، يمكن استعمال قاعدة بيانات مراجعة الكتب في موقع «آمازون» كمفتاح للتعرف ولو بصورة جزئية، إلى الهويات المغفلة في قاعدة بيانات عن المشتريات بواسطة بطاقات الائتمان.

استناداً إلى معلومات عامة لا تأتي على ذكر الهوية، في الإحصاء السكاني في أميركا للعام 1990، استطاعت المختصة في علوم الكمبيوتر لاتانيا سويني أن تتعرف إلى هوية 87 ٪ من سكان الولايات المتحدة، ما يساوي 216 مليوناً من أصل 248 مليون شخص، بواسطة الربط بين أرقام المناطق البلدية المخصصة للأفراد، مع قواعد بيانات عن نوعهم الجنسي وتواريخ ميلادهم. في نصف تلك الحالات، كان يكفي الانطلاق من اسم المدينة، البلدة، أو البلدية، للوصول إلى معرفة الهوية الفردية⁽⁶³⁾. واستطاع بحاثه آخرون التوصل إلى نتائج مماثلة⁽⁶⁴⁾، استناداً إلى بيانات الإحصاء السكاني للعام 2000.

ومع قاعدة بياناته الهائلة عن جمهور الإنترنت، يستطيع محرك البحث «غوغل» التعرف إلى الهويات الفردية في قاعدة بيانات عن المشتريات بواسطة الإنترنت، أو الأسماء في قاعدة بيانات طبية عن الجمهور العام. ويستطيع التجار الذين يحتفظون بمعلومات تفصيلية عن الزبائن ومشترياتهم، استخدام تلك المعلومات في التعرف إلى هويات الأفراد في قواعد البيانات الكبرى لأي محرك للبحث، ولو بصورة جزئية. وكذلك يستطيع سمسار للمعلومات يحوز قواعد بيانات لمجموعة من الشركات، التوصل إلى معرفة الهويات الفردية في معظم سجلات تلك القواعد، بواسطة مقارنتها بعضها بعضاً.

توصل باحثون إلى معرفة هوية الأفراد استناداً إلى معلومات عن أحماض وراثية لا تتضمن هويات أصحابها⁽⁶⁵⁾، بمقارنة تلك المعلومات مع بيانات من مواقع التحري عن الأصول العائلية والعرقية وغيرها. وحتى بيانات البحوث النفسية-الجنسية التي أجراها ألفرد كينزي⁽⁶⁶⁾ في ثلاثينيات القرن الماضي وأربعينياته لم تعد مأمونة. وعلى الرغم من الجهود المضنية التي بذلها كينزي في إخفاء هوية المشاركين في تلك البحوث، استطاعت الباحثة راكيل هيل التعرف إلى هويات 97 ٪ منهم في العام 2013.

ربما لا تبدو تلك الأمور متوافقة مع البداهة العامة والحس السليم⁽⁶⁷⁾، لكن لا يستلزم الأمر سوى قليل من البيانات (أقل مما نعتقد بكثير) للتوصل إلى تحديد الهوية الفردية لمعظم الناس. وعلى الرغم من أننا نبذو عاديّين تماماً، فإننا فريدون جداً. ومثلاً، تبين أنه إذا جرى حذف الأفلام المئة الأكثر مشاهدة، يظهر أن عادات مشاهدة الأفلام هي فردية تماماً. ينطبق أمر مماثل على عادات قراءة الكتب بواسطة الإنترنت، عادات المكالمات الهاتفية، عادات التفتيش على المعلومات بواسطة الشبكة، والشراء بواسطة الـ «ويب». من المستطاع التعرف إلى فرادتنا بواسطة علاقاتنا⁽⁶⁸⁾. ومن الواضح أنه يمكن التعرف إليك تحديداً بواسطة «البيانات المكانية» عنك. ومع معلومات تنسكب على مدار الساعة من هاتفك الخلوي عن أمكنتك، من المستطاع التوصل إلى اسمك من دون عناء كبير. الأرجح أنه لا توجد حاجة لكل تلك المعلومات، إذ يمكن تحديد 95 ٪ من الأميركيين بالاسم استناداً إلى 4 نقاط تقاطع للبيانات عن الوقت والتاريخ ومواقع الأمكنة⁽⁶⁹⁾.

تبدو الإجراءات المضادة المباشرة ضد تلك الأمور غير فعالة على نحو مؤسف. إذ جعلت بعض الشركات مجموعات من بياناتها مغفلة الهوية بإزالة بعض المعلومات منها، وتغيير تذييلات الوقت، أو تعتمد إدخال أخطاء مقصودة في أرقام الهوية التي وضعتها بديلاً للأسماء الفعلية. وسرعان ما تبين أن تلك المناورات لم يكن من شأنها إلا جعل عملية الكشف عن الأسماء الحقيقية أكثر صعوبة بقليل⁽⁷⁰⁾.

واستناداً إلى تلك الأسباب جميعها، تكون القوانين التي تركز على «المعلومات المعرفة بالشخصية» غير مجدية⁽⁷¹⁾. وفي العادة، تشمل تلك المعلومات الاسم، رقم حساب متمتع بالفراة وما إلى ذلك؛ إضافة إلى قوانين مرتبطة بذلك النوع من المعلومات. في المقابل، تتعلق «المعلومات المعرفة بالشخصية» بكمية البيانات أيضاً، فكلما زادت المعلومات التي يعرفها شخص عنك، حتى لو غابت عنها هويتك، زادت فرص أن يتعرف إليك بسهولة أكبر.

في معظم الأحوال، تتمحور حماياتنا حول سياسات الخصوصية في الشركات التي نتعامل معها، لكنها لا تتعلق بالتقنية والرياضيات. ولا يجدي كثيراً استبدال الهوية برقم فريد خاص بها. إذ لا يحول ذلك دون الاستمرار في جمع عمليات جمع المعلومات ومقارنتها واستخدامها، وفي نهاية المطاف يرجح أن يبدّر عنا تصرف ما يؤدي إلى الربط بين اسمنا وملف معلوماتنا «المغفل الهوية».

في عصر الرقابة الكلية القدرة المتسمة بأن الكل يجمع المعلومات عنا طوال الوقت، تضحى الخصوصية هشة تماماً. ويفترض بنا إما اللجوء إلى تقنيات أكثر متانة في الحفاظ على الخصوصية، أو التخلي عن فكرة الحماية بأكملها.

4

تجارة الرقابة

تشكل قدرة الهواتف الحديثة على الإتيان بأشياء مضافة عدّة إحدى الأشياء الأشد إثارة للدهشة. لا يرتدي الناس ساعات لأن هواتفهم فيها ساعة. لا يحمل الناس كاميرات لأنها صارت مكوناً معيارياً في معظم الهواتف الذكية.

من المستطاع أيضاً استعمال ومضات «فلاش» كاميرا الخلوي، لصنع نظام إشارة ضوئي. يعمل التطبيق الرقمي «برايتست فلاش لايت فري» (Brightest Flash Light Free) ⁽¹⁾، على «فلاش» الهواتف التي تعمل بنظام الـ «أندرويد»، وهو تطبيق صنعته شركة «غولدن شورز» (GoldenShores). يعمل التطبيق بشكل جيد، ويتضمن مجموعة من الميزات الجذابة. وذهبت بعض المراجعات عن ذلك التطبيق إلى التوصية بوضعه في متناول الأطفال عندما يتسلون بأحد ألعاب الاختباء والمراوغة. هناك ميزة في التطبيق لم تتناولها المراجعات الكثيرة عنه، هي أنّه يجمع باستمرار بيانات عن مكان مستخدمه ⁽²⁾، مع إمكانية مفترضة بيعها لمُعلنين.

فعلياً، حال التطبيق «برايتست فلاش لايت فري» هي أكثر تعقيداً من ذلك. إذ تعتمد سياسة الخصوصية فيه، بغض النظر عن قلّة من يقرؤها، على مخادعة المستخدمين بفعالية. وتنص على أن الشركة تستطيع استخدام المعلومات التي يجمعها التطبيق، لكنها تتجنب ذكر إمكانيّة بيعها إلى جهات أخرى. وعلى الرغم من أن المستخدمين يجب عليهم أن يضغطوا على زر «أوافق» بالنسبة لاتفاقية السماح

باستخدام التطبيق، تبدأ عملية جمع المعلومات عن موقع المستخدم وإرسالها إلى الشركة، حتى قبل الضغط على ذلك الزر.

أثار الأمر دهشة معظم الـ 50 مليون مستخدم للتطبيق، عندما كشف خبراء عنه في العام 2012⁽³⁾. وتدخلت «اللجنة الفيدرالية للتجارة» في المسألة⁽⁴⁾، مجبرة الشركة على كشف ممارساتها المخادعة وحذف البيانات التي جمعتها. لكن اللجنة لم تفرض غرامة على الشركة؛ لأن التطبيق كان مجانياً.

تخيل لو أن الحكومة الأميركية سنت قانوناً يلزم مواطنيها جميعهم بحمل أجهزة تتبع. في تلك الحال، سيعدُّ القانون فوراً مخالفاً للدستور. ومع ذلك، فإننا ندأب على حمل هواتفنا معنا في الأماكن كلها. إذا أجبرت قوات الشرطة على إبلاغها كلما عقدنا صداقة جديدة، ستثور الأمة بأكملها. ومع ذلك، فإننا نبلغ ذلك إلى «فيسبوك». إذا طلب جواسيس البلاد نسخاً عن مكالماتنا الهاتفية ومراسلاتنا البريدية كلها، سيرفض الشعب الانصياع. لكننا نقدم نسخاً عن رسائلنا الإلكترونية كلها لمن يقدم لنا خدمة الـ «إيميل»، وشركات الخلوي، ومنصات التواصل الاجتماعي، ومقدمي خدمات الإنترنت.

تحدث نسبة ضخمة من الرقابة على يد الشركات، وهي تحدث ذلك بذريعة أننا نوافق عليها. لا أقصد بذلك أننا نتطلع ثم نتخذ قراراً بالموافقة، بدلاً من ذلك تأتي موافقتنا إما لأننا نعطي قيمة للخدمة التي نحصل عليها، أو لأن صفقة متكاملة قُدمت إلينا تتضمن الرقابة⁽⁵⁾، لكننا لا نملك خياراً حقيقياً حيالها. تلك هي الصفقة التي عرضتها في المقدمة.

يتناول هذا الفصل مسألة رقابة الإنترنت علينا، لكن لتذكّر أيضاً أن الأشياء كلها متصلة بالإنترنت، أو أنها ستصبح قريباً كذلك. إن رقابة الإنترنت هي تعبير مختصر عن الرقابة في عالم يتربط بعضه بعضاً بواسطة الإنترنت.

يشكل الإعلان التجاري الهدف الرئيس لكل ما تستهدفه الشركات من رقابة الإنترنت. ثمة سوق جانبي صغير في ذلك المضمار، وكذلك خدمات الزبائن، لكن تلك النشاطات كلها تبدو أمراً هامشياً بالمقارنة مع هدف بيع الأشياء للجمهور.

بصورة تقليدية، تستند رقابة الإنترنت على شيء ما يسمى «الكعكات المحلاة» أو «كوكيز» (Cookies). يبدو الاسم مسالماً وحيداً، لكن الوصف التقني له بأنه «المُعَرَّف الدائم» هو أشد دقة بما لا يقاس. في الأصل، لم يقصد من الـ«كوكيز» أن تكون أدوات للرقابة، بل صُمِّمت كي تجعل الإبحار بواسطة الإنترنت أكثر سهولة. وليس من طبيعة مواقع الانترنت أن تتذكرك عند كل زيارة وكل طريقة على الـ«ماوس». قدّمت الـ«كوكيز» حلاً لتلك المعضلة. تحتوي كل «كوكي» على رقم فريد يتيح للموقع التعرف إليك. وبذا، كلما تجوّلت في موقع للشراء على الإنترنت، كأنك تدأب على القول: «أنا المستخدم صاحب الرقم 608431». ويتيح ذلك للموقع العثور على حسابك عليه، والاحتفاظ ببطاقة للمشتريات ملتصقة بك، وتذكرك عندما تزور الموقع ثانية وهكذا دواليك.

سرعان ما أدركت شركات الإنترنت أن بوسعها الوصول بالـ«كوكيز» الخاصة بها إلى صفحات على مواقع شبكية أخرى، ما أدى إلى ولادة ظاهرة «كوكيز من طرف ثالث». وشرعت شركات كـ«دوبل كليك» (Click Double) ⁽⁶⁾ - اشتراها محرك البحث «غوغل» عام 2007 - في تتبّع مستخدمي الإنترنت أثناء تنقلهم بين المواقع المختلفة. وعند تلك النقطة، صار بإمكان الإعلانات ملاحقتك بواسطة شبكة الـ«ويب» كلها. فتش بواسطة الإنترنت عن سيارة معينة، أو بلدة لقضاء الإجازة فيها، أو وضع صحيّ معيّن؛ ولسوف تستمر بعدها في تلقي إعلانات من شركة تلك السيارة أو البلدة أو شركة الدواء المتعلّق بالوضع الصحي الذي أجريت بحثاً عنه.

وتطوّر الأمر لاحقاً إلى تركيب رقابي خانق بامتداده وقوّته وربحيته. ثمة كثير من الرقابة التي تلاحقك أينما ذهبت أثناء وجودك على الإنترنت، وهي تأتي من الشركات وسفاسرة البيانات: هناك عشرة منها على ذلك الموقع، وعشرون على موقع آخر وهكذا دواليك. يلاحقك «فيسبوك» في المواقع كلها بواسطة زر «لايك» (سواء دخلت إلى حسابك على «فيسبوك» أم لا). ويتابعك «غوغل» في كل موقع يحتوي على زر «غوغل +» (Google+) أو يستعمل أداة التحليل الإحصائي «غوغل أناليتكس» (Google Analytics)، لقياس حركة الزوار عليه.

تملك معظم الشركات التي تلاحقك على الإنترنت ⁽⁷⁾ أسماء ربما لم تسمع بها: «روبيكون بروجكت» (Rubicon Project)، «آد سونار» (Ad Sonar)، «كوانكاست» (Quancast)، «بالس 260» (Pulse 260)، «أندرتون» (Undertone)، «ترافك ماركت بلايس» (Traffic Market Place). إذا أردت أن ترى من يلاحقك ⁽⁸⁾، أضف إلى محرّك البحث الذي تستعمله إحدى الأدوات الرقمية التي تتيح لك رصد الـ «كوكيز» التي تلاحقك. أضمن لك أنك ستفزع. إذ اكتشف أحد المراسلين الصحفيين أن 105 شركات مختلفة لاحقته أثناء استعماله الإنترنت لمدة 36 ساعة ⁽⁹⁾. في العام 2010، زرعت شركة لا تثير الريبة، «دكشينري.كوم» (Dictionary.com)، ما يزيد على 200 «كوكيز» لكل من زار موقعها ⁽¹⁰⁾.

لا يختلف الأمر على هاتفك الذكي. وهناك، تلاحقك التطبيقات أيضاً. وترصد التطبيقات أمكتك، وأحياناً تنقل إليها «دفتر العناوين» في هاتفك الخلوي، ومفكرتك، والمواقع التي وضعت إشارة عليها، وتاريخ عمليات البحث. في العام 2013، توافق مغني الـ «راب» جاي-زي وشركة «سامسونغ» (Samsung) على أن يقدم لمن ينزلون تطبيقاً رقمياً معيناً، فرصة الاستماع إلى ألبومات جاي-زي قبل إطلاقها في السوق. ويشترط ذلك التطبيق عند وضعه على الخلوي ⁽¹¹⁾، الحصول على كل الحسابات الموجودة على الهاتف، وتتبع مواقع أمكتته، ومعرفة الأشخاص الذين يتصل بهم مستعمله. وذهب تطبيق رقمي عن لعبة «العصافير الغاضبة»

«أنغري بيردز» / (Angry Birds)، إلى حد طلب مواقع الأمكنة، حتى عندما لا يبارس المستخدم تلك اللعبة⁽¹²⁾.

وتفرض الشركات التي تقدّم خدمة الاتصال بالإنترنت بالموجات العريضة النطاق «برودباند» (Broad Band) كـ«كومكاست» (Comcast)، رقابة مستمرة على مستخدميها⁽¹³⁾. وتنشغل الشركة حاضراً في معرفة إذا ما كنت تحصل على نسخ غير مرخصة من الأغاني وأشرطة الفيديو، لكن الشركات الأخرى ليست بعيدة كثيراً عن تلك الممارسة. إذ تعمل «مايكروسوفت» و«فريزون» (Verizon) وغيرهما⁽¹⁴⁾، على صنع جهاز لاتصال التلفزيون بالإنترنت، يستطيع أن يرصد ما يجري في الغرفة كي تتخذ من تلك المعلومات قاعدة للإعلانات التجارية.

لا يشبه الأمر وجود «الأخ الكبير»^(*) الأوروبي⁽¹⁵⁾، بل هو أقرب إلى وجود بضع مئات من الإخوة الوشاة الصغار.

وحاضراً، صارت رقابة الإنترنت أكثر صرامة من الـ«كوكيز». واقعياً، ثمة سباق تسلح صغير في ذلك المضمار. محرّك البحث الذي تستعمله -نعم، بما في ذلك «غوغل كروم» (Google Chrome) - يملك ضوابط قويّة بإمكانه وقف عمل الـ«كوكيز»، ويعمد عدد من الناس إلى تفعيل تلك الضوابط. يعدّ برنامج «دونت تراك مي» (DoNotTrackMe) من أشهر الإضافات الإلكترونية التي يمكن إلحاقها بمحرّكات البحث. ورد صنّاع رقابة الإنترنت على ذلك البرنامج وأمثاله بأن صنعوا «فلاش كوكيز» - هي تتألّف أساساً من ملفات تشبه الـ«كوكيز» ويُحْتَفَظُ بها ضمن برنامج «آدوبي فلاش بلاير» (Adobe Flash Player) الذي يتعامل مع ملفات الـ«بي دي أف» والمواد المرئية - المسموعة. وبذا، تبقى الـ«فلاش كوكيز» حتى بعد أن تتخلص محرّكات البحث من الـ«كوكيز» التي ألصقت بها. وللتصدي لذلك

(*) «الأخ الكبير» هو الديكتاتور الحاكم في دولة شموليّة تراقب الجميع، في رواية الكاتب الإنكليزي جورج أورويل 1984.

النوع من الـ«كوكيز»، تستطيع اللجوء إلى برنامج «فلاش بلوك» (FlashBlock). ولكن، هناك طرق أخرى كي تستفرد بك الرقابة⁽¹⁶⁾، بواسطة برامج تحمل أسماء شيفرّة كـ «إيفر كوكيز» (evercookies)، و«كانفاس فنغر برنتنغ» (canvas fingerprinting)، و«كوكيز سينكينغ» (cookies synching). ولا يقتصر الأمر على المسوّقين. ففي العام 2014، توصّل باحثون إلى أن موقع «البيت الأبيض» استخدم الـ«كوكيز» متعدّياً على سياسته بالذات بشأن الخصوصية. سأقدم بعض النصائح بخصوص صدّ رقابة الـ«ويب» في الفصل 15.

كجزء من طبيعتها، تخفي الـ«كوكيز» هويّات من تتعامل معهم، لكن الشركات تربط بينها وبين معلومات أخرى تفيد في التعريف عن هويّاتنا بشكل حاسم. إذ أنت تعرّف عن نفسك طواعيّة لعدد من خدمات الإنترنت. وغالباً ما تفعل ذلك باستخدام اسم مستخدم خاص بك، لكن سرعان ما يغدو مستطاعاً الربط بين اسمك فعلياً وأسماء المستخدم التي تستعملها. حاول «غوغل» فرض ذلك بواسطة ما سمّاه «سياسة الاسم الحقيقي»⁽¹⁷⁾، بمعنى الطلب من مستخدمي «غوغل +» التسجيل فيه بأسمائهم القانونيّة، لكنه ألغى تلك السياسة في 2014. إلى حدّ بعيد، يطلب «فيسبوك» الاسم الحقيقي⁽¹⁸⁾. وعندما تستخدم بطاقتك الائتمانيّة في شراء شيء ما، يجري ربط هويّتك الحقيقيّة بـ«كوكيز» تعطيك الشركة التي تتعامل معها. وفي كل مرّة تستخدم هاتفك الخليوي للدخول إلى الإنترنت، يجري الربط بينك كمالك للخليوي مع عملية البحث، على الرغم من أن المواقع الشبكيّة ربما تجهل ذلك.

مجاني ومريح

تشكّل الرقابة نموذج الأعمال التجاريّة على الإنترنت، لسببين رئيسين: ميل الناس إلى المجاني، وانجذابهم أيضاً إلى ما هو مريح. على الرغم من ذلك، تبقى حقيقة أن الناس ليس لديهم خيار فعليّ. وتمثّل الحال في أنّه إما الرقابة أو عدم

الحصول على شيء؛ ولكون الرقابة غير منظورة، وهو أمر مريح، فليس عليك التفكير بها. وغدت الأمور كلها ممكنة لأن القانون الأميركي لم يتطور ليواكب المتغيرات في ممارسة الأعمال التجارية.

قبل العام 1993، كانت الإنترنت غير تجارية بالمرّة، والمجاني هو العرف السائد على الشبكة. عندما وصلت بواكير الأعمال التجارية إلى الشبكة، ثار كثير من النقاش عن طريقة جعلها مدفوعة. وسرعان ما تبين أنه، فيما عدا حالات استثنائية معزولة كالاستثمار المباشر والمواقع الإباحية جنسياً، لا يرغب الناس في دفع ولو قليل من المال مقابل الوصول إلى خدمات الشبكة⁽¹⁹⁾. وبما يشبه كثيراً نموذج الأعمال التجارية على التلفزيون، شكّلت الإعلانات النموذج الوحيد للحصول على مردود مجزٍ، ومكّنت الرقابة من جعل الإعلان مربحاً أكثر. وبات بإمكان المواقع الشبكية أن تفرض رسوماً أعلى على الإعلانات الموجهة بصورة شخصية، من تلك التي تحصلها مقابل البث العام للإعلانات. وعلى ذلك النحو، وصلنا إلى وضع تسود فيه نُظُمٌ مجانية اسمياً، وهي تجمع بياناتنا وتبيعها مقابل ما تقدّمه لنا من خدمات، ثم تقصفنا بالإعلانات.

يمثّل «المجاني» سعراً له طبيعة خاصة به⁽²⁰⁾، كما أثبتت بحوثٌ عدّة أنّ الناس لا تتفاعل معه بصورة منطقية. إذ نميل إلى الإغلاء من قيمة ما هو مجاني. نضغط على آخرين كي يستخدموه. يطوّق المجاني حسناً الطبيعي حيال مسألة التناسب بين الكلفة والمنفعة، ثم ينتهي الأمر بالناس إلى بيع بياناتهم الشخصية بأقل من قيمتها.

يتضاعف ذلك الميل إلى تقليل قيمة الخصوصية لأن الشركات تسعى إلى التأكد من ألا تكون أمراً بارزاً عند جمهور المستخدمين. عندما تدخل إلى «فيسبوك»، أنت لا تفكر في كمية المعلومات الشخصية التي تقدّم إلى الشركة، بل تفكر في أنك تتحدث مع أصدقائك. عندما تستيقظ صباحاً، أنت لا تفكر في أنك بصدد السماح لحفنة من الشركات بأنّ تتبعك طيلة النهار، بل تكتفي بأن تدس الخلوي في جييبك.

وتتجسد النتيجة في أن شركات الإنترنت تستطيع تحسين عروضها للشركة الفعليين، بتهوين قيمة خصوصية المستخدم. يمارس موقع «فيسبوك» ذلك الأمر منهجياً منذ سنوات⁽²¹⁾، بواسطة تحديثه بانتظام سياسته في الخصوصية بهدف الحصول على مزيد من الوصول إلى بياناتك، وإعطائك مقداراً أقل من الخصوصية. وكذلك بدّل «فيسبوك» سياسته حيال الأمور الأساسية في خلفية الإعدادات⁽²²⁾، بما يمكن مزيداً من الناس من رؤية اسمك، وصورتك، وتديونتك، والصور التي تضعها على صفحتك، والأشياء التي ضغطت زر «لايك» عليها وما إلى ذلك. فعل محرك البحث «غوغل» أموراً مشابهة كثيرة⁽²³⁾. ففي العام 2012، أعلن «غوغل» تغييراً أساسياً قوامه أنه سيصنع مجموعة معلومات موحدة يربط فيها بياناتك التي تأتيه من عمليات التفتيش، بريد «جي ميل»، موقع «يوتيوب» (الذي اشتراه «غوغل»)، «غوغل+» وغيرها.

في ذلك المضمار، تكاد شركة «آبل» أن تكون استثناءً⁽²⁴⁾. إذ تتعامل الشركة مع أسواق السلع الاستهلاكية، ولكن على الرغم من أنها تستطيع التجسس على البريد الإلكتروني في قاعدة بياناتها المسماة «آي كلاود» (iCloud)، والرسائل النصية، والمفكرات، ودفاتر العناوين، والصور؛ فإنها تحجم عن ذلك الأمر. وتستعمل المعلومات عن عمليات الشراء في مخزنها الشبكي «آي تيونز» (iTunes)⁽²⁵⁾، وبصورة حصرية، لمجرد اقتراح أغاني أخرى وأشرطة فيديو مختلفة ربما يرغب المستخدم في شرائها. ومنذ العام 2014، شرعت في استخدام ذلك الملمح باعتباره صفة تنافسية مميزة لها في السوق.

تشكل الراحة السبب الثاني في كوننا نسلّم طوعياً بياناتنا الشخصية جداً إلى مصالح الشركات، ونصبر على تحويلنا أشياء نخضع لرقابتها. ومثلما أقول تكراراً، إنّ الخدمات المستندة إلى الرقابة هي مفيدة وقيمة. إذ نسعد لكوننا قادرين على الوصول إلى دفاتر العناوين، والمذكرات، والصور، والوثائق، والأشياء الأخرى كافة، أينما كنّا وبواسطة أي جهاز يكون متاحاً لنا. يعجبنا وجود خدمات كمحركي البحث

«سيري» (Siri) و«غوغل ناو» (Google Now)، وهما يتألقان في عملهما كلما كان بحوزتهما أظنان من المعلومات عنك. تسهل تطبيقات شبكات الـ«سوشال ميديا» مسألة الاتصال مع أصدقائنا. تزداد فعالية أداء تطبيقات خلوية كـ«خرائط غوغل» و«ييلب» و«ويزر» (Weather) و«أوبر»، كلما زادت معرفتها بالأمكنة التي نكون فيها. ويبدو سمحنا لتطبيقات كـ«بوكيت» (Pocket) و«إنستاباير» (Instapaper)، بمعرفة عاداتنا في المطالعة، ثمناً قليلاً مقابل الحصول على معظم ما نرغب في قراءته متجمعاً في المكان نفسه. وربما نسر أيضاً عندما تصلنا إعلانات موجهة تحديداً إلى ما نهتم به. إنّ المكاسب المتحصلة من الرقابة في تلك التطبيقات وغيرها، هي فعلية ومؤثرة.

وعلى نحو خاص، لا نمانع أن تجمع الشركات معلومات عنا وتستخدمها في تحسين خدماتها كي تكون خدمة أكثر بالنسبة لنا. ويفسر ذلك أن شكاوى الناس بشأن رقابة الشركات، لا تتضمن غالباً توصيات بشأن موقع «آمازون». فبصورة مستمرة، يقدم لنا ذلك الموقع نصائح تستند إلى ما نشتره، وما اشتريناه ماضياً، وما اشتراه آخرون أيضاً. وبذا، يستعمل «آمازون» بياناتك بطريقة تجميعها نفسها، ويكون فائق الشفافية مع المستخدم في ذلك الشأن. إنها تجارة ضخمة لـ«آمازون»، وتلقى قبولاً واسعاً لدى الجمهور⁽²⁶⁾. ولكن، يبدأ الناس بالشكوى عندما تباع بياناتهم وتشتري وتستعمل، من دون علمهم وبلا إذن منهم.

صناعة اسمها: سمسرة المعلومات

ترجع رقابة الزبائن إلى عهود سابقة على عصر الإنترنت بكثير. فقبل ذلك العصر، وُجِدَت 4 تيارات رئيسة للرقابة. تأتي التيار الأول من احتفاظ الشركات بسجلات عن زبائنهم. كان المثل على ذلك هو شركة للإمداد بمتطلبات التصنيع تحتفظ بسجلات عن طلبات زبائنهم من المؤسسات، ومن هم الذين يقومون بالطلبات فعلياً. كان ذلك عهداً تتذكر فيه شركة «نوردستروم» (Nordstrom)

للحياكة، أحجام زبائنهم ونوعية الخياطة التي ينجذبون إليها، وتحفظ فيه شركات الطيران والفنادق بسجلات عن زبائنهم الدائمين. بالنتيجة، تطوّرت تلك الأمور كلها لتصنع قاعدة بيانات تمكّن الشركات من تتبع مسارات مبيعاتها بداية من الطلبية الأولى وانتهاءً بالشراء فعلياً، وبطاقات ولاء الزبائن التي تمنح حسومات للمستهلك لكن غاياتها الفعلية كانت تقصي مشترياتهم. وحاضراً، تمنح شركات كثيرة نظماً تعرف باسم «إدارة العلاقة مع الزبون» (اختصاراً، «سي آر إم» CRM)، إلى المؤسسات من الأحجام كافة.

جاء التيار الثاني من الرقابة التقليدية، بواسطة التسويق المباشر. شكّل البريد الورقي واسطتها، فيما تمثّل الهدف في إمداد الشركات بقوائم لأسماء من يرغبون في تلقي بريد تسويقي، وعدم تبديد الرسائل على أناس لا يرغبون في تلقيها. كانت تلك العملية تقريبية بالضرورة؛ لأنها استندت إلى أشياء كالمعلومات الديموغرافية، أو اشتراكات المجلات، أو قوائم الزبائن من شركات السلع المختلفة.

وأتى التيار الثالث من مكاتب الائتمان. إذ دأبت تلك الشركات على جمع معلومات ائتمانية عن الناس، ثم بيع المعلومات إلى بنوك تريد اتخاذ قرار بشأن إعطاء زبائنهم قروضاً، وكذلك معدلات الفوائد عليها. ونسبياً، كان ذلك نوعاً مكلفاً من عمليات جمع المعلومات الشخصية، ولا تكون مجدية إلا إذا تعلق الأمر بكميات كبيرة من النقود: إعطاء بطاقات ائتمان، والسماح لشخص ما باستئجار شقة وما إلى ذلك.

جاء التيار الرابع من الحكومات. وتكوّن من السجلات الحكومية بأنواعها: شهادات الميلاد والوفاة، سجلات رخص السواقة، قوائم الناخبين، الشهادات والرخص المتنوعة وهكذا دواليك. وبأطراد، صار باستطاعة الشركات أن تشتري تلك البيانات العامة، أو تنزلها بواسطة الإنترنت من المواقع الحكومية⁽²⁷⁾.

جمعت مكاتب الائتمان وشركات التسويق المباشر تلك التيارات الأربعة كي تصبح شركات لسماسة المعلومات، التي هي حالها حاضراً على غرار شركة «أكزيوم»⁽²⁸⁾. تشتري تلك الشركات⁽²⁹⁾ بياناتك من الشركات التي تتعامل معها، ثم تربطها مع معلومات أخرى عنك، ثم تبيع البيانات الناتجة عن تلك العمليات إلى شركات تريد معرفة مزيد من المعلومات عنك. وركبت شركات سماسة المعلومات موجات الأتمتة والانتقال إلى عصر الكمبيوتر. وكلما زادت كمية المعلومات التي تنتجها أنت بنفسك، تمكنت تلك الشركات من جمع مزيد من البيانات، مع رفع قدرتها على صنع ملف شخصي دقيق عنك⁽³⁰⁾.

يشير الدهشة حقاً ما تتمتع به معلومات سماسة البيانات من السعة والعمق⁽³¹⁾. إذ يجمع أولئك السماسرة معلومات ديموغرافية كالأسماء، العناوين، أرقام الهاتف، عناوين البريد الإلكتروني، النوع الجنسي، العمر، الحال العائلية، وجود أطفال في الأسرة، المستوى التعليمي، المهنة، مستوى الدخل، الانتماء السياسي، السيارات، ومعلومات عن المنازل والملكيات وغيرها. ويجمعون أيضاً قوائم عن مشترياتك، وتاريخ الشراء وطريقة الدفع.

وكذلك يتبعون حالات الطلاق، والوفيات والأمراض في عائلتك. ويجمعون كل شيء عما تفعله على الإنترنت⁽³²⁾.

ويستخدم سماسة البيانات المعلومات عنك كي يصفوك في فئات قابلة للتسويق⁽³³⁾. هل تريد قوائم عن يندرجون في فئات «وارث محتمل» أو «بالغ يعيل أبويه العجوزين»، أو عناوين الأسر التي «تركز على مرض السكري» أو «حاجات المسنين»؟ تستطيع شركة «أكزيكوم» إمدادك بتلك القوائم كلها⁽³⁴⁾. باعت شركة «إنفو إس إيه» (InfoUSA) قوائم عن «مسنين قيد المعاناة» و«مسنين تسهل مخادعتهم»⁽³⁵⁾. في 2011، باعت إحدى شركات سماسة البيانات، اسمها «تلتراك» (Teletrack)، قوائم عن تقدموا بطلبات عن مكونات ائتمانية غير مألوفة

كقروض الدفع اليومي، إلى شركات كانت تسعى لعقد صفقات مالية سيئة مع مثل أولئك الأشخاص. في 2012، باعت شركة السمسة «إيكوفاكس» (Equifax) قوائم المتخلفين عن دفع أقساط رهوناتهم، لشركات تقدّم ديوناً منخفضة الفائدة. ولأن ذلك الأمر تعلّق ببيانات مالية، فرضت «المحكمة الفيدرالية للتجارة» غرامات مالية على «إيكوفاكس» والشركات التي اشترت قوائمها أيضاً⁽³⁶⁾. في ما عدا ذلك، بدت الأمور الأخرى كأنها تسير بعدالة تامة.

الإعلانات الشخصية

نستعمل نظماً تتجسّس علينا لقاء الحصول على خدمات⁽³⁷⁾. وحاضراً، تسير أمور الإنترنت على هذا النحو. إذا كان شيء ما مجانياً، فأنت لست المستهلك⁽³⁸⁾؛ بالأحرى أنت المنتج. ووفق تعبير آل غور، المرشح السابق للرئاسة في أميركا: «لدينا اقتصاد يبحث عن طرائد»⁽³⁹⁾.

ودوماً، عانت الإعلانات من مشكلة أن معظم من يشاهدونها لا يهتمون بالمنتجات التي تعرضها. يعدُّ تبديداً أن تقدّم إعلاناً عن البيرة لمن لا يتناولها. ينال التبديد معظم الإعلانات عن السيارات، إلا إذا كنت في سوق للسيارات. ولكن، مع استحالة توجيه الإعلانات بطريقة إفرادية، تصرّفت الشركات بأحسن الطرق بالبيانات الموجودة لديها. إذ قسّمت الناس جغرافياً، ووضعت أفضل التخمينات عن المجالات والبرامج التلفزيونية الأكثر قدرة على جذب مستهلكين محتملين. لقد تتبعوا السكان بعمومهم، أو بتقسيمهم إلى مجموعات ديموغرافية كبرى. اتّسمت تلك الأمور كلها بغيباء الفعالية. ثمة قول مشهور غالباً ما ينسب إلى جون وانا مايكر، قطب مبيعات التجزئة: «أعلم أن نصف إعلاني هي تبديد تام. وتكمن المشكلة في أنني لا أعرف أي نصف منها هو كذلك»⁽⁴⁰⁾.

تملك الرقابة الشاملة الكلية القدرة إمكانية تغيير ذلك الأمر. إذا كنت تعرف بالضبط من يرغب في شراء جزّارة للعشب أو من يقلق بشأن ضعف الانتصاب⁽⁴¹⁾،

يغدو باستطاعتك توجيه إعلانك إلى الشخص المناسب في الوقت المناسب، مع عدم تبديد أي شيء. (فعلياً، تستخدم شركة لرعاية الحدائق⁽⁴²⁾ تعمل على مستوى أميركا كلها صوراً جوية كي تروج لإعلاناتها بشكل أفضل). وإذا علمت التفاصيل الكاملة عن مستهلك محتمل - بما فيها نوع الحجج التي تقنعه، وأنواع الصور المرغوبة لديه - تغدو إعلاناتك أشد فعالية.

ينطبق الوصف عينه على الإعلان السياسي، بل غير فعلياً طريقة إدارة الحملات السياسية⁽⁴³⁾. استخدم باراك أوباما «البيانات الضخمة» و«الإعلان الشخصي» في حملتيه الرئاسيتين عامي 2008 و2012⁽⁴⁴⁾، ويسير على منواله مرشحون من الطيف السياسي بأكمله. تستخدم تلك البيانات في توجيه جهود التمويل والرسائل السياسية الفردية⁽⁴⁵⁾، والتأكد من ذهابك إلى صناديق الاقتراع يوم الانتخاب؛ مع افتراض أن قاعدة البيانات تشير إلى أنك ستصوت للمرشح المناسب لأصحابها.

تكتظ بيانات الرقابة التجارية بأخطاء متنوعة⁽⁴⁶⁾، لكنها تكون مفيدة⁽⁴⁷⁾ حتى عندما لا تكون دقيقة تماماً. فحتى لو وصل بك الأمر إلى إيصال ثلث إعلاناتك إلى أشخاص لا يجدي استهدافهم بها، تكون قد أدت حملة إعلانية فعالة حقاً. لا يكمن وجه الأهمية في الدقة الكاملة لتوجيه الإعلانات، بل في كون المعلومات أصبحت أفضل بكثير مما كانته في الماضي⁽⁴⁸⁾.

في العام 2013 مثلاً، استطاع باحث أن يحدّدوا الأمكنة الجغرافية لأشخاص يستعملون «تويتر»، بتحليل تشابهاتهم مع مستخدمين آخرين لـ «تويتر»⁽⁴⁹⁾. لم يكن معدل الدقة مرتفعاً لديهم - إذ بلغت 58 ٪ عند تحديد المدينة التي كان فيها المستخدمون - لكن تلك النسبة تعدُّ أكثر من كافية بالنسبة لعدد كبير من شركات الإعلانات التجارية.

على الرغم من ذلك، تتوافر أدلة كثيرة على أن الإعلانات المستندة إلى الرقابة تُباع بسهولة⁽⁵⁰⁾. هناك قيمة لإبراز الإعلانات إلى أناس يرغبون بها، خصوصاً عندما

تصلهم في اللحظة التي يكونون فيها بصدد اتخاذ قرار الشراء. يحاول «غوغل» فعل ذلك بالضبط بواسطة خدمة «آد ووردز» (Adwords) التي تضع الإعلانات قرب نتائج عمليات البحث. ويحاول الأمر عينه باعة التجزئة على الإنترنت بواسطة الإعلانات التي تقول «الذين اشترؤا هذا الشيء، اشترؤوا تلك الأشياء أيضاً». لكن تلك الأشياء تستند إلى قليل من الرقابة.

ليس واضحاً ما هي كمية المعلومات التي تعدُّ كافية. هناك أهمية لمعرفة معلومات شخصية عامة عن الناس: مثليو الجنس، المقبلون على الزواج، الذين يفكرون في قضاء عطلة في مناطق دافئة، الذين لديهم مستوى معين من الدخل. وتعطي شركة للسيارات قيمة كبيرة لمعرفة تفيدها بأنك ترغب في سيارة عائلية وليس سيارة بسقف متحرك، لكنها لا تقيم وزناً كبيراً لمعرفة تفضيلك أن تكون السيارة زرقاء أو خضراء. وكذلك الحال للمعلومة التي تقول إن لديك طفلين، أحدهما ما زال بحاجة إلى كرسي طفل على المقعد الخلفي، أو أن أحد الطفلين قضى أثناء حادث تحطم سيارة⁽⁵¹⁾. صحيح أن وكيل البيع سيحاول إقناعك بشراء سيارة أكبر في الحال الأولى (لديك طفلان)، وبمعايير السلامة في الثانية (طفل قضى في حادث سيارة)، لكن الفارق في العائدات سيكون ضئيلاً باستمرار. وكذلك ربما يثير الإعلان المشخص بدقة نوعاً من الريبة، ما يهدد بانصراف الزبون عن الشراء⁽⁵²⁾.

في هذا المضمار، يفيد تذكر مفهوم يأتي من عوالم الروبوت. إذ نرتاح للتعامل مع الروبوتات التي تبدو لنا كروبوتات منذ النظرة الأولى، وكذلك تلك التي تشبه البشر تماماً. لكننا لا نشعر بالراحة مع روبوت يشبه الناس كثيراً، لكنه لا يكون بشرياً تماماً. أشار عالم الروبوت الياباني ماساهيرو موري إلى تلك الظاهرة باسم «الوادي غير الخادق»⁽⁵³⁾. ولفتت سارة دبليو. واطسون، وهي من نقاد التكنولوجيا، إلى وجود ظاهرة مماثلة في عالم الإعلان. إذ يرتاح الناس إلى إعلانات تحمل طابعاً شخصياً موارباً⁽⁵⁴⁾، وكذلك الحال مع الإعلان الذي يكون طابعه الشخصي مرهفاً

وغير ملموس، لكنهم ينفرون من إعلان «مريب» نسبياً فيه ما يوحي بأنه يتلاعب بهم أو يكون غير متطابق مع نظرهم لأنفسهم.

سوف يتغير ذلك كله مع الزمن، عندما نعتاد على الإعلان الشخصي. الحال أن تعريف «المريب» نسبي وسيّال⁽⁵⁵⁾، ويعتمد كثيراً على مدى ألفتنا مع التكنولوجيات موضع البحث⁽⁵⁶⁾. حاضراً، تكون مريبة تلك الإعلانات التي تتبعنا أثناء تجوالنا بواسطة الإنترنت⁽⁵⁷⁾. ويمكن للمريب أن يصحّح نفسه بنفسه. يملك «غوغل» تاريخاً طويلاً ومعقداً مع الإعلانات التي لا يسمح لها بأن تترافق مع عمليات البحث عليه؛ لأن مستخدميهم وجدوا أنّ بعض أنواع الإعلانات تثير إحساساً بالريبة لديهم. وتسمح شركات أخرى للمستخدمين بالنقر على وصلة إلكترونية تفيد في تعريفهم بسبب ملاحظتهم من قبل إعلان معين⁽⁵⁸⁾. ويهدف ذلك إلى جعلهم أكثر ألفة مع عملية الإعلان الشخصي.

من الناحية الثانية، تكتفي شركات بإخفاء الأمر. بعد القصة التي وردت آنفاً عن تمكّن شركة «تارغت» من التعرّف إلى حمل مراهقة كانت تخفيه عن أبيها^(*)، غيرت الشركة أسلوب إرسال الإعلانات الشخصية إلى الناس. إذ لم تتوقّف عن إرسال إعلانات للنساء اللواتي تخمّن أنهن حوامل، لكنها دسّتها ضمن إعلانات أكثر عمومية. لم تشعر اللواتي وصلتهن تلك الإعلانات بواسطة الـ «إيميل» أنهن مستهدفات على نحو شخصي، لذا أحسسن بريبة أقل حيالها⁽⁵⁹⁾.

في الوقت عينه، يؤدّي تكاثر الإعلانات حولنا إلى التقليل من قيمة الإعلانات الفردية، لسببين على الأقل: أولاً، مع تشبّع عالمنا بالإعلانات، tend to lose their value as individual advertisements. ويرجع ذلك إلى أن كمية النقود التي ننفقها لا تتغير. مثلاً، تنصّارح شركات السيارات كلها على الربح المتأتي من السيارة الواحدة التي تشتريها.

إذا رأيت عشرات أضعاف الإعلانات، يكون لكل منها عُشر القيمة؛ لأنك لن تشتري في ختام المطاف سوى سيارة واحدة.

ثانياً، من السهل علينا تماماً إبعاد الإعلانات عنا. منذ رواج أشرطة الفيديو التقليدية في منتصف السبعينيات من القرن العشرين، تنبّه المعلنون إلى أهمية الشكل الذي تبدو عليه إعلاناتهم عندما يستخدم الناس زر «إلى الأمام بسرعة»، كي يقفّزوا عن مشاهدتها. خاضت شركات الإعلانات الشبكية معركة أكثر تعقيداً بهدف الاستحواذ على اهتمامنا.

في البداية كانت تلك الإعلانات مجرد لوحات تظهر في أعلى صفحات الإنترنت. وعندما تعلّمنا أن نتجاهلها، شرعت في تبني طريقة الومض مع إظهار شرائط الفيديو الرقمية. وحاضراً، صارت الإعلانات متداخلة كثيراً مع ما نريد قراءته، ما يلجئنا إلى تعمد إبعادهم عن أبصارنا. ويقدر أن ما يزيد على 50 مليون شخص، وضعوا برنامج «آدبلاك بلاس» (AdBlock Plus) ⁽⁶⁰⁾ الذي يصدّ الإعلانات في محرّكات البحث.

وبالنتيجة، تنخفض قيمة الإعلان الشبكي المفرد باطراد ⁽⁶¹⁾، على الرغم من الارتفاع المستمر في تكلفة الإعلان بواسطة الإنترنت. ووفقاً لذلك، تدنّت بسرعة قيمة بياناتنا بالنسبة للمعلنين. قبل بضع سنوات، كان الملف الشخصي التفصيلي عن كل فرد يحوز قيمة كبيرة، وحاضراً يحوز عدد كبير من الشركات وسامسة البيانات تلك المعلومات، ما جعلها سلعة عادية ⁽⁶²⁾. في سياق تحليل تقارير مالية في 2013، ورد أن قيمة البيانات عن الفرد تصل إلى 42 دولاراً سنوياً على محرّك البحث «غوغل» ⁽⁶³⁾، لكنها مجرد 6 دولارات في «فيسبوك»، وشبكة «لينكدن» (LinkedIn) المهنية ومتصفّح «ياهو» (Yahoo!). وللسبب عينه، لا يكف موقع «غوغل» و«فيسبوك» عن رفع لواقطها. إذ يحتاجان إلى مزيد ومزيد من المعلومات عنا كي يبيعاها للمعلنين، وبالتالي يتأيان بنفسيهما عن المنافسة.

من المحتمل أننا وصلنا نقطة الذروة⁽⁶⁴⁾، ما يعني أن الربحية من مردود الإعلانات سوف تشرع في الانحدار، ما يوصلها إلى وضع تكون فيه غير قادرة على الاستمرار كنموذج وحيد للعمل. لا أظن أن أحداً يعرف كيف ستبدو عليه الإنترنت إذا انفجرت فقاعة إعلاناتها⁽⁶⁵⁾، وأضحى التسويق بواسطة الإعلانات المستندة إلى الرقابة غير مجدٍ، واضطرت شركات الإنترنت إلى العودة للأسلوب القديم في الأعمال: أن تفرض رسوماً على مستخدميها.

قوة الوسطاء الجدد

تمثلت إحدى «الكليشيات» المبكرة للإنترنت في أنها سوف تنهي الشركات الوسيطة⁽⁶⁶⁾. لن تعتمد على الصحف التي تستعرض الأخبار اليومية وتقدمها لك في حزمة ورقية قابلة للقراءة بسهولة. فعلى الإنترنت، تستطيع أن تصمم الصحيفة التي ترغب فيها، وتأخذ تنقاً من هنا وهناك كي تصنع ما تريده تحديداً. وعلى نحو مماثل، لن تعتمد على المخازن الكبرى في البيع والتسوق، سوف يعمل موقع «إي باي» (eBay) المختص بالتجارة الإلكترونية على ربط الباعة بالشراسة مباشرة⁽⁶⁷⁾. وسارت الأمور على النحو نفسه بالنسبة للترويج والتوزيع في الموسيقى⁽⁶⁸⁾ وتذاكر الطيران⁽⁶⁹⁾، وفي بعض الأحيان، الإعلانات التجارية⁽⁷⁰⁾. ساد اعتقاد بأن النماذج السابقة في الأعمال اعتمدت على قدامى «حراس البوابات»^(*)، والإنترنت غيرت تلك الآليات كلها.

يصح الأمر حاضراً بأكثر مما كانه قبلاً. إذ يتيح موقع «إربن بي» للأفراد التنافس مع الفنادق التقليدية. ويسهّل موقع «تاسك رابت» الاتصال بين الأشخاص الذين يريدون القيام بأعمال غير مستساغة مع الناس الذين يسعون إلى العثور على من ينفذ لهم أعمالاً غير مستساغة. وتلغي مواقع «إي باي» و«إيتساي» و«كافيه-برس» الحاجة إلى أسواق بيع الأشياء المستعملة. يتجاوز موقعي «زيلو» و«ريدفن»

(*) إشارة إلى الدور الذي يؤديه الوسطاء، سواء أكانوا أفراداً أم شركات.

أعمال السماسرة العقاريين، وكذلك يفعل موقع «إي ترايد» بالنسبة لمستشاري الاستثمارات، وينطبق ذلك على ما يفعله موقع «يوتيوب» بشبكات التلفزة. ويلغي موقع «كريغ ليست» الحاجة إلى التحقيقات الصحافية، ويفعل موقع «هوت واير» و«ترافيلوسيتي» الأمر عينه بالنسبة لوكلاء السفر.

ربما نجحت الشركات الشبكية الجديدة في كسر مراكز القوة التقليدية للمتاجر الكبرى، والصحف، وشركات التاكسي؛ لكن تحكمها في سريان المعلومات بين الشراة والباعة أوصلها إلى تأديتها هي نفسها دور الوسطاء الأقوياء. وأمام ناظرينا، بات السوق مساحة لمعركة بين الوسطاء القدماء والجدد. إذ تتصارع «آبل» ومخزنها «آي تيونز» مع الصناعة التقليدية للموسيقى، ويتواجه «آمازون» مع دور النشر التقليدية، و«أوبر» (Uber) مع شركات سيارات الأجرة. ويكسب الوسطاء الشبكيون الجدد تلك المعركة باستمرار.

عبر إيريك شميدت، المدير التنفيذي لـ «غوغل»، عن ذلك بوضوح قائلاً⁽⁷¹⁾: «نعتقد أن منصات التقنيات الحديثة كـ «غوغل» و«فيسبوك» و«آمازون» و«آبل»، هي أشد قوة مما يعتقد كثيرون... وما يمنحهم تلك القوة قدرتهم على النمو، تحديداً قدرتهم على رفع كمية أعمالهم بأضعاف مضاعفة، بسهولة وسرعة فائقة. لا شيء، ربما ما عدا الفيروسات البيولوجية، يستطيع فعل ذلك بسرعة تلك المنصات التكنولوجية وكفاءتها وقوتها، وهو أيضاً ما يجعل من يصنعون تلك المنصات ويديرونها ويستعملونها، أقوياء تماماً».

تشير كلمات شميدت إلى الطبيعة الاحتكارية المتأصلة في الوسطاء الشبكيين الجدد. هناك مجموعة متنوعة من التأثيرات الاقتصادية التي تكافئ من ينطلق أولاً⁽⁷²⁾، وتعاقب من يدخل المنافسة متأخراً، وتربط الناس بالشبكات الأكثر ضخامة، ما يجعل من الصعب عليهم الانتقال إلى نُظم منافسة. ونتيجة لذلك، يحوز

أولئك الوسطاء الشبكيون الجدد قوة أكبر مما امتلكه الوسطاء القدماء الذين حلّ الجدد بديلاً منهم.

إذ يتحكّم «غوغل» بثلاثي سوق عمليات البحث على الإنترنت⁽⁷³⁾. وأنشأ ثلاثة أرباع مستخدمي الإنترنت حسابات لهم على «فيسبوك»⁽⁷⁴⁾. ويتحكّم موقع «آمازون» بقرابة 30 ٪ من سوق الكتب في الولايات المتحدة⁽⁷⁵⁾، وتحوز شركة «كومكاست» قرابة 25 ٪ من سوق الاتصال بالإنترنت⁽⁷⁶⁾، بواسطة الموجات العريضة النطاق [«برودباند»] (Broad Band). تملك تلك الشركات قوة هائلة، وتتحكّم بنا ببساطة استناداً إلى مستوياتها الاقتصادية.

تجمع تلك الشركات كلها بياناتنا كي تزيد من هيمنتها على السوق وربحياتها في الأعمال. عندما انطلق موقع «إي باي» للتجارة الإلكترونية، كان من السهل على الشراء والبيعة أن يتحاوروا خارج نظام «إي باي»؛ لأن عناوين البريد الإلكتروني للأفراد كانت متاحة للعموم.

في العام 2001، شرع «إي باي» في إخفاء عناوين البريد الإلكتروني⁽⁷⁷⁾، وفي 2011، حظر وضع عناوين البريد الإلكتروني والوصلات الإلكترونية في القوائم⁽⁷⁸⁾، وفي 2012، حظرت تلك المعلومات في التراسل بين مستخدم وآخر⁽⁷⁹⁾. خدمت تلك التحركات كلها أن يصبح «إي باي» وسيطاً قوياً بتصعيبه عمليات إنشاء صلات بين الباعة والشراء داخل نظام «إي باي»، ثم نقلها إلى خارجه.

وباطّراد، تستخدم الشركات قوتها للتأثير في مستخدميها والتلاعب بهم. تبذل المواقع الشبكية التي تستفيد من الإعلانات جهوداً مكثفة للتأكد من قضائك أطول وقت ممكن عليها⁽⁸⁰⁾، بتعديل محتوياتها كي تصبح جذابة إلى حدّ إدمانها. وتلجأ القلة من المواقع التي تسمح لك بالخروج من إعلاناتها الخاصة إلى تصعيب عملية

الوصول إلى ذلك الخيار⁽⁸¹⁾. وبمجرد أن تتمكن الشركات من المزج بين تلك التقنيات والمعلومات الشخصية، تضحي النتائج أعمق غوراً وأشد خفاءً وتراكمية. لا تعتمد علاقاتنا مع مجموعة كبيرة من شركات الإنترنت على النموذج التقليدي لعلاقة الشركة بالزبون. ويرجع ذلك أساساً إلى أننا لسنا مجرد زبائن بالأحرى، نحن منتجات تباعها تلك الشركات إلى زبائننا/الحقيقيين. إنها أقرب إلى العلاقات الإقطاعية من كونها علاقات تجارية⁽⁸²⁾. تشبه شركات الإنترنت السادة الإقطاعيين، ونحن رعاياهم توابعهم وفلاحهم، بل نكون- في يوم سيء- خدَمَهم. نحن مزارعون مستأجرون بالنسبة لتلك الشركات، إذ نعمل في أراضيها وننتج معلومات تتولى بيعها للحصول على أرباح.

نعم، تمثل الكلمات السابقة مجازاً؛ لكن الأمور تكون كذلك غالباً. أقسم بعض الناس يمين الولاء لـ «غوغل». إذ ينشؤون حساباً على بريد «جي ميل» الإلكتروني، ويستخدمون «وثائق غوغل» و«مفكرة غوغل»، كما يحملون هواتف تعمل بنظام الـ «آندرويد» الذي صنعه «غوغل». وأقسم آخرون يمين الولاء لـ «آبل». إذ يملكون حواسيب من نوع «ماك- آبل»، وهواتف «آي فون»، وألواح «آي باد» الإلكترونية، ويسمحون لموقع «آي كلاود» بالاحتفاظ بنسخ عن أشياءهم كلها، مع تحديثها كلما جدّ جديد. وما زال بعضنا يسمح لـ «مايكروسوفت» بتولي الأمور كلها. وهجر شطر كبير منا البريد الإلكتروني ليتكل كلياً على «فيسبوك»، و«تويتر» و«إنستغرام». ربما نفصل سيّداً إقطاعياً على غيره. ربما نوزع ولاءنا على عدد من تلك الشركات، أو نثابر على تجنب شركة ننفر منها. بصرف النظر عن ذلك كله، بات من الصعب عدم الولاء على الأقل لواحد من أولئك السادة.

في نهاية المطاف، يحصل الزبائن على منافع كثيرة من الولاء لسادة الإقطاعيين. ببساطة، من الأسهل والأكثر مأمونية أن يتولى شخص آخر حفظ بياناتنا وإدارة أجهزتنا. إذ نرغب أن يتولى شخص آخر العناية بإعدادات أجهزتنا وضبطها⁽⁸³⁾،

وإدارة البرامج فيها، وتخزين المعلومات عليها. ونرغب في الوصول إلى بريدنا الإلكتروني من كل الأمكنة التي نكون فيها، ومن كل كومبيوتر يتوافر لنا؛ وكذلك نحب أن يكون «فيسبوك» بتصرفنا، فندخله من كل الأجهزة وفي الأمكنة كلها. ونريد أن تظهر التحديثات التي نضيفها على مفكراتنا، بأجهزتنا كلها. تتفوق علينا المخازن الرقمية الضخمة لـ «سُحُب المعلومات» في تخزين صورنا وملفاتنا؛ وأدت «آبل» عملاً عظيماً بأن حمت المخزن الرقمي لتطبيق «آي فون» من البرمجيات الخبيثة. نحب تلقي تحديثات أمنية لحماية أجهزتنا، والاحتفاظ بنسخ أوتوماتيكية عن ملفاتنا؛ فالشركات أفضل منا تماماً في حماية أجهزتنا. ونشعر بالسعادة عندما نرى معلوماتنا كلها تظهر دفعة واحدة بكبسة زر، إذا فقدنا هاتفنا الذكي واشترينا آخر بديلاً عنه.

في العالم الجديد للحوسبة، لم يعد منتظراً منا أن ندير بيئة معلوماتنا الإلكترونية. نضع ثقتنا بأن يحسن السادة الإقطاعيون معاملتنا ويحمونا من الأذى. تنجم تلك الأمور كلها من مسارين في التكنولوجيا:

يتمثل المسار الأول في صعود تقنية «حوسبة السحاب» (Cloud Computing) ⁽⁸⁴⁾. وبصورة أساسية، تفترض تلك التقنية بأن المعلومات لم تعد تخزن وتدار من أجهزتنا الخاصة؛ بل تحدث الأمور كلها في خوادم ضخمة تملكها مختلف الشركات المعلوماتية. النتيجة؟ نفقد السيطرة على معلوماتنا. تدخل تلك الشركات على معلوماتنا وبياناتنا- يشمل ذلك المحتوى و«البيانات الوصفية» معاً- خدمة لأي هدف ربحي تريده. وبحرص، صاغت الشركات بنود الخدمة، وهي تمل أنواع البيانات التي نستطيع تخزينها على نُظُم الشركات، ما يمكنها من حذف حساباتنا بأكملها إذا ارتأت أنه يخالف تلك البنود. وتقدم معلوماتنا إلى جهات إنفاذ القانون، من دون معرفتنا ولا موافقتنا ⁽⁸⁵⁾. أسوأ من ذلك، ثمة إمكان لأن تخزن بياناتنا في كومبيوترات موجودة في بلاد لا تتمتع بقوانين قوية لحمايتها.

يتمثل الميل الثاني في صعود أجهزة المستخدم⁽⁸⁶⁾، التي تستمر الجهات البائعة في إدارتها على نحو وثيق بعد بيعها. يشمل ذلك أجهزة «آي باد»، و«آي فون»، وهواتف الـ «آندرويد»، و«كيندل»، و«كروم بوكس» وغيرها. وبالنتيجة، لم نعد نسيطر على بيئة الحوسبة الإلكترونية، بأجهزتها وأدواتها وملفاتها. لقد سلّمنا إلى الشركات الزمام في كل ما نقدر أن نراه ونفعله ونستخدمه. تفرض شركة «آبل» قوانين⁽⁸⁷⁾ بشأن أنواع البرامج والتطبيقات التي يمكن وضعها على الأجهزة التي تعمل بنظام التشغيل «آي أو إس» الذي تملكه. وتستطيع أن تضع وثائق الخاصة على جهاز «كيندل» للقراءة الإلكترونية، لكن مالكنه «آمازون» تستطيع أن تحذف كتباً باعتها هي بنفسها لك. في العام 2009، حذفت «آمازون» أوتوماتيكياً نسخاً من رواية الكاتب جورج أورويل 1984 من أجهزة «كيندل»⁽⁸⁸⁾؛ بسبب قضايا تتعلق بالملكية الفكرية. وبمرارة، أعرف أنه لم يعد ممكناً كتابة أعمال روائية ماثلة.

حتى النظامين الكبيرين في تشغيل الكومبيوترات، «ويندوز 08» (Windows 08) من «مايكروسوفت» و«يوزمايت» (Yosemite) من «آبل»، يسيّران في ذلك الاتجاه عينه.

وتضغط كل من الشركتين على المستخدمين كي لا يشترروا سوى تطبيقات مجازة منها، ولا تباع سوى في مخازنها الرقمية المركزية. ويزيد الشبه بين كومبيوتراتنا وهواتفنا الذكية، مع كل تحديث لنُظّم التشغيل فيها.

لا يتعلق الأمر بالأجهزة وحدها. لم تعد طليق اليد في شراء أي برنامج ترغب فيه، وتضعه على كومبيوترك. وباطّراد، تتجه الشركات البائعة إلى تبني نموذج الاشتراك⁽⁸⁹⁾ - فعلت ذلك شركة «آدوبي» (Adobe) الشهيرة، عند إطلاقها سحابة «كرييتيف كلاود» (Creative Cloud)⁽⁹⁰⁾ في 2013، التي تعطي الشركة البائعة سلطات كبيرة. لم تتخل «مايكروسوفت» كلياً عن نظام البيع، لكنها جعلت الاشتراك في برنامج «أوفيس» مغرياً تماماً. ومن الصعب مقاومة ما يعرضه «أوفيس

365) (Office 365) لجهة تخزين الوثائق في «سحابة المعلومات» التي تديرها «مايكروسوفت». تعمل الشركات على دفعنا في ذلك الاتجاه؛ لأنه يجعلنا ندر أرباحاً أكثر، كمستخدمين وزيائن.

في ظل القوانين السارية حاضراً، تشكل الثقة خيارنا الوحيد. ليس ثمة قوانين منسجمة أو قابلة للتوقع. لا سلطة لنا على أفعال تلك الشركات. لا أستطيع أن أتفاوض بشأن حق متصفح «ياهو» في الوصول إلى صوري على موقع «فليكر» (Flickr) المخصص لصور الأفراد. لا أستطيع تطلب مزيد من الحماية لشرائح العروض الضوئية الخاصة بي، عندما أضعها على موقع «بريزي» (Prezi)، ولا قوائم الأشياء الواجب علي إنجازها عندما أضعها على موقع «تريلو» (Trello). ولا أعرف حتى أسماء الشركات التي أناط بهم مقدمو خدمة «سحابة المعلومات»، لإنجاز البنية الإلكترونية التحتية لتلك الخدمة. إذا حذفت تلك الشركات بياناتي، لا أملك حتى الحق في طلب استرجاعها. لا خيار لي في الأمر برمته. وإذا قرّرت ترك تلك الخدمات، فالأرجح أنني لن أتمكن بسهولة من أخذ معلوماتي وبياناتي معي⁽⁹¹⁾.

لاحظ العالم السياسي هنري فاريل⁽⁹²⁾ أن «معظم حياتنا بات يجري بواسطة الإنترنت. ويقول آخر، صار معظم حياتنا يجري بموجب قوانين تفرضها شركات القطاع الخاص، وهي لا تخضع لكثير من القوانين الحكومية ولا للمنافسة التقليدية في السوق الفعلي».

ثمة دفاع يتكرّر حيال ذلك الأمر، من نوع «الأعمال هي الأعمال». لا أحد مجبر على الانضمام إلى «فيسبوك»، أو استخدام عمليات البحث في «غوغل»، أو الشراء بواسطة الـ «آي فون». ينخرط المستخدمون طوعاً في تلك العلاقات الشبيهة بالإقطاعية، بسبب ضخامة ما يحصلون عليهم من خدمات لقاء ذلك. إذا لم يعجبهم الأمر، ليتوقفوا عنه.

تلك النصيحة ليست عملية. ليس من المنطقي القول للناس⁽⁹³⁾ إنه إذا لم تعجبهم عمليات جمع المعلومات والبيانات، سيكون عليهم التوقف عن استعمال البريد الإلكتروني، أو التسوق بواسطة الإنترنت، أو استخدام «فيسبوك» أو امتلاك خلوي. لا أستطيع تخيل أنه بمقدور الطلبة إنهاء مراحل تعليمهم بعد الآن، من دون استعمال محرّكات البحث على الإنترنت أو موسوعة «ويكيبيديا»، ولا العثور على وظيفة بعد ذلك. إنها أدوات الحياة الحديثة.

إنها أدوات ضرورية للمهن والحياة الاجتماعية. لا يمثل الخروج منها خياراً قابلاً للحياة⁽⁹⁴⁾، بالسنة لغالبينا؛ لكنها في معظم الأوقات تنتهك ما باتت أعرافاً فعلية في الحياة المعاصرة.

وكذلك لا تمثل المفاضلة بين مقدّمي الخدمات الإلكترونية اختياراً بين الرقابة أو عدمها، بل مجرد خيار للسيد الذي يتجسّس عليك.

5

الرقابة والسيطرة الحكوميتان

ربما يصعب فهم المدى الكامل الذي تصله الرقابة الحكومية. سأركز على حكومة الولايات المتحدة، ليس لأنها المعتدي الأسوأ، بل لأننا نعرف شيئاً ما عن نشاطاتها؛ أساساً بفضل أعمال مشكورة لإدوارد سنودن.

تتميّز رقابة الأمن القومي في الولايات المتحدة بأنها مكيّنة سياسياً وقانونياً وتقنياً. كشفت وثائق سنودن⁽¹⁾ عن وجود ثلاثة برامج على الأقل، تملكها «وكالة الأمن القومي» لجمع المعلومات عن كل مستخدم لبريد «جي ميل». تستند تلك البرامج الثلاثة إلى ثلاث قدرات تقنية في التنصّت. وكذلك فإنّها تعتمد على ثلاث سلطات قانونية مختلفة، وتشتمل على تعاون ثلاث شركات مختلفة. تلك هي الصورة بشأن «جي ميل» وحده. وينطبق توصيف مشابه بصورة شبه مؤكّدة على الشركات الكبرى كافة التي تقدّم خدمة البريد الإلكتروني، سجلات الهواتف الخلوية، «البيانات المكانية» لتلك الهواتف، ومحادثات الإنترنت.

من أجل فهم دور الرقابة في الاستخبارات الأميركية، يجب فهم تاريخ مهمة «وكالة الأمن القومي» في التنصّت العالمي، والتغيّر في طبيعة الجاسوسية. بسبب ذلك التاريخ، تمثّل «وكالة الأمن القومي» المنظّمة الرئيسة للتنصّت بالنسبة للحكومة الأميركية.

تأسست «وكالة الأمن القومي» على يد الرئيس هنري ترومان في العام 1952⁽²⁾، الذي جمع الاستخبارات الأميركية لنظم الإشارة ونشاطات كسر الشيفرات ضمن منظمة واحدة⁽³⁾. وكانت المنظمة وما زالت جزءاً من الجيش الأميركي، واستهلت عملها بوصفها منظمة مختصة كلياً في جمع المعلومات عن الاستخبارات الأجنبية.

وتزايدت أهمية تلك المنظمة أثناء الحرب الباردة بين أميركا والاتحاد السوفياتي. وحينها، كان التلصص على الاتحاد السوفياتي هو العرف السائد، وكانت الاستخبارات الإلكترونية جزءاً من ذلك، ثم زادت أهميتها عندما صارت الأعمال كلها تجري بواسطة الكمبيوتر، كما باتت الاتصالات الإلكترونية أكثر شيوعاً. وزادت كمية المعلومات التي نجمعها مع تنامي قدراتنا وزيادة كمية الاتصالات التي يجب تجميعها.

وعلى رغم عدم جدوى معظم تلك الأشياء، فإن بعضها كان مفيداً تماماً. وواضح تماماً أن الوصول إلى الأسرار عن الواقع⁽⁴⁾ - على غرار ميزات دبابة سوفياتية جديدة - هو أكثر سهولة من الوصول إلى ألباز النوايا، من نوع الخطوة التالية التي يرغب الرئيس السوفياتي نيكيتا خروتشوف القيام بها. لكن، أولئك كانوا أعداءنا، وجمعنا كل شيء تمكنا من جمعه عنهم.

كان من الواجب تقليص تلك المهمة المتفرّدة مع سقوط الشيوعية في أواخر الثمانينيات من القرن العشرين وبداية تسعينياته، كجزء من حصص السلام. لبرهة، سرى ذلك الأمر، وتنامت أهمية المهمة الأخرى لـ «وكالة الأمن القومي» المتمثلة في حماية الاتصالات الأميركية من تجسس الآخرين. باتت «وكالة الأمن القومي» أشد تركيزاً على الشؤون الدفاعية، وأكثر انفتاحاً. لكن أعمال التنصت اكتسبت حياة جديدة أشد كثافة، عقب هجمات الإرهاب في 9 / 11. «لن تتكرر أبداً». مثل ذلك الشعار التزاماً مستحيلاً بالطبع⁽⁵⁾، لكن الطريق الوحيد لمنع أي شيء من الحدوث

هو معرفة كل ما يحصل. وأدى ذلك بـ «وكالة الأمن القومي» إلى وضع الكرة الأرضية تحت الرقابة.

في أعمال الجاسوسية التقليدية، تتواجه الحكومات مع بعضها بعضاً. ونتجسّس على الحكومات الأجنبية والأشخاص الذين يكونون عملاء لها. لكن، كان العدو مختلفاً في حال الإرهاب. لم يعد الأمر يتعلّق بحفنة من قادة الحكومات «هناك»؛ بل صار خلايا إرهاب عشوائية من المحتمل أن يكون أعضاؤها في أي مكان. ترصد الرقابة الحكومية الحديثة كل شخص، يستوي في ذلك المحلي والدولي⁽⁶⁾.

وليس ذلك للقول إن رقابة الحكومة للشعب هو أمر جديد. إذ فعلته الحكومات التوتاليتارية طيلة عقود في الاتحاد السوفياتي، وألمانيا الشرقية، والأرجنتين، والصين، وكوبا، وكوريا الشمالية وغيرها. في الولايات المتحدة، تجمّست «وكالة الأمن القومي» والـ «إف بي آي» على أميركيين من الأنواع كلها. في ستينيات القرن العشرين وسبعينياته، تجمّست الوكالة على نشطاء معارضة الحرب، قادة الحركة المدنية، وأعضاء مجموعات سياسية سلمية متمردة. في العقد الأخير، أعادت التركيز مجدداً على نشطاء مناهضة الحرب وأعضاء مجموعات سياسية سلمية متمردة، إضافة إلى المسلمين الأميركيين. وتضاعفت أهمية تلك المهمة الأخيرة⁽⁷⁾، بعدما صارت «وكالة الأمن القومي» الوكالة الرئيسة المسؤولة عن ملاحقة «القاعدة» خلف البحار.

ترافق ذلك التغيير في الهدف مع تطوّر في تكنولوجيا الاتصالات. قبل زمن الإنترنت، كان من السهل التركيز على الاتصالات الأجنبية. في شبكة الاتصالات العسكرية الصينية، لم يكن هناك سوى الاتصالات الصينية. استُخدم نظام الاتصالات الروسي من أجل الاتصالات الروسية وحدها. إذا اخترقت «وكالة الأمن القومي»⁽⁸⁾ أحد الكوابل البحرية بين مدينتي «بتروبافلوفسك»

و«فلاديفستوك» الروسيّتين، لم يكن عليها أن تقلق بشأن احتمال أنها اخترقت الاتصالات بين مدينتي «ديترويت» و«كليفلاند» الأميركيّتين.

تعمل الإنترنت بطريقة مغايرة كليّاً. إذ تختلط اتّصالات الناس كلها على الشبكات نفسها. يستخدم الإرهابيّون مقدّمي خدمات البريد الإلكترونيّ، كالأخرين كلهم. وتحمل الدوائر الإلكترونيّة نفسها اتّصالات الحكومات الروسيّة والإيرانيّة والكويّة، متمازجة مع تغريداتك على موقع «تويتر».

وربما تنتهي المكالمات الشبكيّة بين نيويورك و«لوس أنجلوس» إلى كوابل بحرية روسيّة. من المحتمل أن تحوّل المكالمات بين «ريو دي جينيرو» و«لشبونة»، عبر فلوريدا. لا يخزّن «غوغل» بياناتك في مقرّه في «ماونتن فيو»⁽⁹⁾، بل ينشرها في عدد من مراكز تجميع المعلومات عبر العالم: في تشيلي وفنلندا وتايوان والولايات المتّحدة وغيرها. مع تطوّر شبكات الاتّصالات الإلكترونيّة العالميّة، صار من الصعب عدم جمع المعلومات عن الأميركيّين، حتى لو لم يكونوا هم الأهداف المطلوبة.

في الوقت نفسه، شرع الجميع في استعمال البرامج والأجهزة نفسها. سابقاً، كانت الأجهزة الإلكترونيّة والراديو والكمبيوتر في روسيا تعمل بتقنيّات روسيّة. لم يعد ذلك موجوداً؛ إذ نستخدم جميعنا نظام «ويندوز- مايكروسوفت»، والمحولات الشبكيّة لشركة «سيسكو»، ومنتجات الأمن الإلكترونيّ نفسها. تستطيع شراء هاتف «آي فون» في معظم البلدان. يعني ذلك أن الإمكانات التقنيّة لاختراق الشبكات العسكريّة الصينيّة أو نُظُم المكالمات الهاتفية الفنزويليّة مثلاً، قابلة للتعميم عالميّاً.

تحوز الولايات المتّحدة أوسع شبكة للرقابة في العالم بفضل ثلاث ميزات. تملك الميزاتيّة الأضخم للاستخبارات⁽¹⁰⁾؛ إذ تفوق مجموع نظيراتها في الدول كلها. وتؤدّي طبيعة تمديدات شبكة الإنترنت فعليّاً إلى مرور معظم الاتّصالات العالميّة بحدود الولايات المتّحدة⁽¹¹⁾، حتى لو كانت بين بلدين مختلفين. وتضم أراضي

الولايات المتحدة معظم الشركات الكبرى للإنترنت، وتلك التي تصنع البرامج والأجهزة الأكثر شعبية وانتشاراً؛ وهي بالتالي تسير تحت القوانين الأميركية. إنها المهيمن في ذلك المضمار.

وبجلاء، يتلخّص هدف رقابة «وكالة الأمن القومي»⁽¹²⁾، وفق الاقتباسات التي تظهر في شرائح العروض الضوئية فائقة السريّة على موقعها الشبكي، في: «اجمع كل شيء»، و«اعرف كل شيء»، و«استفد من كل شيء». «تخترق» وكالة الأمن القومي الإنترنت لدى شركات الاتصالات للهواتف والكوابل، كما تجمع البريد الإلكتروني، والرسائل النصيّة، وتاريخ عمليات البحث بواسطة الإنترنت، ودفاتر العناوين، و«المعلومات المكانيّة»، وكل شيء آخر تستطيع وضع يدها عليه.

لا يوجد دليل على أن «وكالة الأمن القومي» تجمع المكالمات الهاتفية كلها في الولايات المتحدة⁽¹³⁾، لكننا نعلم أنها تفعل ذلك في أفغانستان وبرمودا (على الأقل)⁽¹⁴⁾، تحت مظلة برنامج «سومالغيت» (SOMALGET). بلغت ميزانية الوكالة قرابة 10.8 بليون دولار في 2013⁽¹⁵⁾، وتوظف مباشرة قرابة 33 ألف شخص⁽¹⁶⁾، إضافة إلى أعداد أخرى ممن يعملون معها بوصفهم متعاقدين⁽¹⁷⁾. كانت إحدى وثائق سنودن هي «الميزانية السوداء» الفائقة السريّة، لـ «وكالة الأمن القومي» ووكالات استخباراتية أميركية أخرى: إذ بلغ مجموعها 53 بليون دولار في 2013⁽¹⁸⁾. ويقدر أن الولايات المتحدة تنفق 72 بليون دولار سنوياً على الاستخبارات⁽¹⁹⁾.

جاء الكثير من أموال «وكالة الأمن القومي» المخصصة لبنيتها التحتية الرقابية الحديثة من الجهود الحربيّة في أفغانستان والعراق بعد أحداث 9/11. كانت تلك جهوداً هجوميّة للتعرف إلى الأهداف المعادية وتحديد أمكنتها، مع جهود دفاعيّة للتعرف إلى أدوات التفجير البدائيّة والعمل على تفكيكها. يعني ذلك أن قدرات الوكالة تطوّرت بمواجهة شبكات في تلك البلدان⁽²⁰⁾؛ وكذلك لأن كل شخص

على الكرة الأرضية يستخدم المعدات نفسها، صار ممكناً استعمال تلك المعدات ضدّ النُظم في أمكنة مختلفة.

ثمة سؤال يبرز بشكل واضح: هل ذلك العمل قانوني؟ الجواب الحقيقي هو أننا لا نعلم، إذ تأتي السلطة الحالية لـ «وكالة الأمن القومي» من ثلاثة أمكنة:

الأمر التنفيذي رقم 12333⁽²¹⁾، موقعاً من الرئيس رونالد ريغان في 1981، ويميّز للوكالة إجراء رقابة واسعة في الخارج. ويتضمّن بعض الحماية للمواطنين الأميركيين وحدهم⁽²²⁾، لكنه يميّز عمليات واسعة في جمع المعلومات عن الأميركيين وتحليلها والاحتفاظ بها.

الفصل 215 من التشريع الأميركي «قانون باتريوت»⁽²³⁾ (Patriot Act USA) (*) الذي سنّ عام 2001، ويسمح للوكالة بأن تجمع «أي شيء ملموس (بما فيها الكتب والتسجيلات والأوراق والوثائق والمكوّنات الأخرى)» - عن كل شخص، وليس الأجانب وحدهم - «خدمة لتحقيق هدفه في الحماية من الإرهاب الدولي والنشاطات الاستخباراتية السرية». ربما بدت الكلمات الأخيرة كأنها تقييد، لكن محكمة سرية فسرتها⁽²⁴⁾ بطريقة تجعلها تشمل الجمع المستمر لـ «البيانات الوصفية» عن المكالمات الهاتفية لكل أميركي.

الفصل 702 من تعديلات قانون «فيسا» (FISA)⁽²⁵⁾، اختصاراً لعبارة «قانون رقابة الاستخبارات الأجنبية» (Foreign Intelligence Surveillance Act) للعام 2008، وأجاز للوكالة بمفعول رجعي نشاطات لتجميع المعلومات كانت أجرتها بطريقة غير قانونية بعد 9/11. كما وسّع نطاق اختصاص الوكالة بما يسمح لها بجمع المعلومات عن الأجانب، مع وجود حماية ضئيلة تماماً للمواطنين الأميركيين. استخدمت الوكالة تلك السلطة لترصد الهيكل العام لبنية اتصالات الإنترنت أثناء دخولها أميركا، مع حصد البيانات عن الأجانب والأميركيين معاً.

(*) الترجمة الحرفية للكلمات هي "شرعة الأميركي الوطني"

هناك سبب مزدوج لعدم وضع حدّ للنقاش عند هذه النقطة. أولاً، لا يتمتع عدد من تدابير الرقابة التي تضمّنتها تلك القوانين بالدستورية الكافية؛ سواء ما يتعلّق بالتفتيشات أم المصادرات غير الشرعيّة. وثانياً، بعض تفسيرات «وكالة الأمن القومي» لتلك القوانين هي بالتأكيد غير شرعيّة، وتناقش المحاكم حالياً تحدّيات رفعت في وجهه تلك المسالك. اعتقد أنه في النهاية، سوف توقف المحاكم كثيراً مما تفعله الوكالة حاضراً، وكذلك سوف توقف تشريعات جديدة مقبلة كمية أكبر من تلك الأفعال. بالطبع، حينها سيكون الأميركيون قد عانوا عقوداً من الرقابة الواسعة، وهو ما يحتمل أنه استراتيجية الوكالة أصلاً. سوف أناقش ذلك بمزيد من التوسّع في الفصل 13.

تجمع «وكالة الأمن القومي» معلومات كثيرة عن الأميركيين، بعضها يبدو «عرضياً». بقول آخر، إذا راقبت الوكالة شبكة هواتف في فرنسا، فلسوف تجمع معلومات عن مكالمات بين الولايات المتحدة وفرنسا. وإذا ترصّدت كابل بحري للإنترنت في مياه المحيط الأطلسي، فلسوف تحصد معلومات عن أميركيين يصادف أن الحركة الإلكترونية المتصلة بنشاطاتهم جرى تحويلها بذلك الكابل. وهناك قوانين تقليصيّة للوكالة⁽²⁶⁾، هدفها الحدّ من قدرتها على جمع معلومات عن الأميركيين وتحليلها وتخزينها، على الرغم من أن معظم ما علمناه عن تلك القوانين يشير إلى أنها ليست فعالة عملياً. هنالك قوانين مختلفة عن محتوى الاتّصالات من جهة، و«البيانات الوصفية» من ناحية ثانية؛ ويعتمد الفارق في القوانين على السلطة الشرعيّة التي تستند إليها الوكالة في تبرير اختراقاتها. ولا يعني التقليص الوصول إلى حدّ حذف المعلومات عن الأميركيين، بل مجرد حفظ المعلومات مع إغفال الهويّات؛ بانتظار أن يأتي أحد ما ويطلب أن يرى ما هي عليه فعلياً. تمارس الوكالة كثيراً من المخادعة مع القوانين في ذلك المضمار⁽²⁷⁾، وحتى أولئك الذين يحاولون التدقيق في نشاط الوكالة يقرّون بأنهم لا يستطيعون تخيّل ما تفعله الوكالة حقاً.

في 2014، ظهر تحليل عن وثائق قدمها سنودن⁽²⁸⁾، بشأن بعض ما حصلت عليه الوكالة فعلياً في سياق اختراقها الحركة الإلكترونية على الإنترنت. وتبين أن بيانات عن أشخاص أبرياء، أميركيين وغير أميركيين، فاقت تلك التي جُمعت عن أهداف جرى تشريع رقابة الاستخبارات عليها. يعبر الأمر عن بعض من طبيعة عمل الاستخبارات. وحتى المعلومات المقلصة عن شخص ما سوف تحتوي على اتصالات مع أشخاص أبرياء؛ لأن كل اتصال - حرفياً - مع هدف ما، يقدم أي نوع من المعلومات المثيرة للاهتمام؛ سيجري الاحتفاظ به.

ربما تتصدّر «وكالة الأمن القومي» صفحات الجرائد، لكن مجتمع الاستخبارات الأميركية يضم فعلياً 17 وكالة مختلفة. بالطبع، هنالك «وكالة الاستخبارات المركزية» («سي آي إيه»). ربما سمعت عن «نرو» (NRO)، الاسم المختصر لـ «المكتب الوطني للاستطلاع» (National Reconnaissance Office)، ويتولى مسؤولية الأقمار الاصطناعية للبلاد. وهناك وكالة استخبارات لكل من الفروع الأربعة للجيش. وتمارس الرقابة «وزارة العدل» (كلاً من الـ «إف بي آي» و«مكتب مكافحة المخدرات»)، والدولة، والطاقة، والخزانة، و«الأمن الوطني» (Homeland Security)، إضافة إلى بضع وكالات أخرى. ربما يكون هناك الوكالة الـ 18 السرية. (ليس أمراً مرجحاً، لكنه محتمل. إذ بقيت تفاصيل مهمة «وكالة الأمن القومي» سرية حتى سبعينيات القرن الماضي، بعد عشرين سنة من إنشائها).

بعد «وكالة الأمن القومي»، تبدو الـ «إف بي آي» الوكالة الحكومية الأكثر غزارة في ممارسة الرقابة. وتربطها علاقات وثيقة مع «وكالة الأمن القومي»⁽²⁹⁾، ويتقاسم الطرفان المعلومات والتقنيات والسلطات التشريعية. من السهل نسيان أن الوثيقة الأولى لسنودن نشرتها صحيفة الغارديان البريطانية - وكانت كناية عن الأمر الذي صدر لشركة «فريزون» لتسليم «البيانات الوصفية» عن زبائنها كلهم - تضمنت أيضاً أمراً لـ «إف بي آي» بتسليم المعلومات إلى «وكالة الأمن القومي». ونعرف أنه يوجد تشارك كثيف⁽³⁰⁾ في المعلومات بين «وكالة الأمن القومي» و«سي آي

إليه» و«وكالة مكافحة المخدرات» و«وكالة الاستخبارات العسكرية» و«وزارة الأمن الوطني». ويعمل أحد برامج «وكالة الأمن القومي» الذي يحمل اسماً مشفراً هو «أي سي ريتش» (ICREACH)، على إمداد 23 وكالة حكومية بمعلومات عن أميركيين.

وإذ قيل ذلك، وعلى عكس «وكالة الأمن القومي»، تتميز الرقابة التي تمارسها الـ«إف بي آي» بأنها تخضع تقليدياً لمراجعة من السلطة التشريعية، بواسطة عملية الحصول على مذكرات تفتيش قانونية. ووفق التعديل الرابع في الدستور الأمريكي، يجب على الحكومة أن تبرهن لقاض أن عملية التفتيش يمكن أن تكشف أدلة عن جريمة، بطريقة معقولة. في المقابل، تملك الـ«إف بي آي» سلطة أن تتولى جمع، من دون مذكرة قانونية، معلومات شخصية من الأنواع كلها؛ سواء بطريقة موجهة لأفراد أم باستهداف مجموعات كبيرة باستخدامها «رسائل الأمن القومي» التي تتمثل أساساً في مذكرات توقيف تصدرها الـ«إف بي آي» من دون مراجعة قضائية. وجرى توسيع أمدية تلك المذكرات في 2001، بقانون «باتريوت أكت» (الفصل 55 منه)، على الرغم من أن الأسس القانونية الأصلية لتلك الرسائل ترجع إلى العام 1978⁽³¹⁾. وحاضراً، تستعمل الرسائل عموماً في الحصول على معلومات من طرف ثالث: رسائل البريد الإلكتروني في «غوغل»، والسجلات البنكية من المؤسسات المالية، وملفات من موقع «دروب بوكس» (Dropbox).

في الولايات المتحدة، عمدنا إلى تخفيض حقوق الخصوصية على تلك البيانات كلها، بسبب ما يسمّى بـ«مبدأ الطرف الثالث». ففي العام 1976، سرق مايكل لي سميث امرأة في «بالتيمور»، ثم دأب على مضايقتها بالهاتف. وبعدما عثرت الشرطة على شخص تشابه أوصافه مع سميث، طلب من شركة الهاتف إنشاء «سجل مكتوب» عن الخط الهاتفي لسميث، مع تسجيل كل أرقام الهواتف التي يتصل بها. بعد التأكد من أن سميث اتصل بالمرأة، حصلت الشرطة على مذكرة تفتيش لمنزله، واعتُقل سميث بتهمة السرقة. حاول سميث إبطال الأهمية القانونية

لـ«السجل المكتوب» لأن الشرطة لم تحصل على تفويض قانوني بإنشائه. في 1979، قرّرت «المحكمة العليا» أنه لم يكن من الضروري الحصول على تفويض قانوني لإنشاء «السجل المكتوب» عن مكالمات سميث الهاتفية، قائلة: «إن هذه المحكمة رأت باستمرار أن المرء لا حق له بتوقعات قانونية، بشأن معلومات سلّمها طواعية إلى طرف ثالث». وتعني تلك الكلمات أساساً، أنه بسبب مشاركة سميث أرقام الهواتف التي يتحدث إليها مع شركة الهاتف⁽³²⁾، فإنه يفقد الحق في توقع أن تحظى تلك المعلومات بأي نوع من الخصوصية. ربما بدا ذلك منطقياً في 1979، عندما كانت معظم معلوماتنا وبياناتنا تحت سيطرتنا، وقريبة منا. ولكن حاضراً، تتجمع معلوماتنا كلها في «سحابة» لا نعرف مكانها، ويمسك بها مجموعة من أطراف ثلاثة، وهي متفاوتة في درجة الموثوقية.

عزّزت التقنية كثيراً قدرة الـ«إف بي أي» على ممارسة الرقابة من دون الحصول على تفويض قانوني. ومثلاً، تستخدم الـ«إف بي أي» (وكذلك الشرطة المحلية)، أداة إلكترونية تسمى «آي أم أس أي - كاتشر» (IMSI-Catcher)⁽³³⁾ التي هي أساساً برج لاتصالات الخليوي، لكنه زائف. إذا كنت سمعت عن ذلك، فلا بد أنك سمعت عن اسم شيفري هو «ستنغراي» (StingRay)⁽³⁴⁾، وهو عملياً نوع من «آي أم أس أي - كاتشر» يبيعه شركة «هاريس كوربوريشن». وعند تفعيل ذلك البرج، تنخدع به الهواتف الخلوية القريبة منه، فتتصل به. وبمجرد حصول ذلك، يعمل «آي أم أس أي - كاتشر» على جمع بيانات عن أمكنة تلك الهواتف وهوياتها⁽³⁵⁾، بل إنه أحياناً يستطيع التنصّت على المكالمات الصوتية، والرسائل النصية، وعمليات الدخول إلى الإنترنت بواسطة الخليوي. ويستحوذ الذعر على الـ«إف بي أي» بشأن شرح تلك القدرة للجمهور⁽³⁶⁾، إلى حدّ أنها تفرض على الشرطة المحلية توقيع اتفاقيات عن عدم الكشف عنها، قبل استخدام تلك التقنية؛ وتوجّه الشرطة بأنها تكذب بشأن استعمال «آي أم أس أي - كاتشر» في المحاكم⁽³⁷⁾. وعندما بدا أن الشرطة المحلية في مدينة «ساراسوتا» بولاية فلوريدا قد تكشف وثائق معدّات «ستنغراي» القادرة على

اعتراض المكالمات الخلوية المحليّة إلى المدعين في قضية حقوق مدنيّة رفعت ضدهم، صادر الضباط الفدراليون تلك الوثائق⁽³⁸⁾.

يصعب الإحاطة تماماً بالمنظمات الحكومية الأميركية المنخرطة في الرقابة. يحتفظ «المركز القومي لمكافحة الإرهاب»⁽³⁹⁾ بسجل عن «بيئة البيانات المتصلة بهويات الإرهاب كافة»، وهي مؤسسة تشكّل مخزناً لمعلومات الحكومة عن الإرهابيين الدوليين المشتبه فيهم. وفي 2007، كانت المؤسسة تحتفظ بقاعدة بيانات ضخمة عن المواطنين الأميركيين⁽⁴⁰⁾، وتُبقى عينها مفتوحة على قرابة 700 ألف مُعرّف (ما يشبه كونهم أشخاصاً، لكن ليس بالضرورة)، وهي مصدر قوائم الرقابة المختلفة⁽⁴¹⁾. وتبدو عمليّات التعامل مع تلك القوائم اعتباريّة⁽⁴²⁾، وعندما يجري التركيز على أحدهم يصبح كمن لا ملاذ آمن له. كان اسم تاملان تسارنايف، المفجّر في «ماراثون بوسطن»، على إحدى تلك القوائم⁽⁴³⁾.

هناك أيضاً «فرق العمل لدعم مكافحة الجريمة المنظّمة»⁽⁴⁴⁾ الذي يعمل مع التحقيقات المتعلّقة بالمخدرات، و«المبادرة الوطنية الشاملة لأمن الفضاء السبراني»^{(45)(*)}، وهي تتعامل مع التهديدات التي تطال الحواسيب. ويعمل «مكتب الكحول والتبغ والأسلحة النارية» على بناء قاعدة معلومات ضخمة بهدف تتبع الناس وأصدقائهم⁽⁴⁶⁾. وحتى البنتاغون مارس التجسّس على الأميركيين⁽⁴⁷⁾، بواسطة وكالة لا تحظى بشهرة واسعة اسمها «النشاط لمكافحة التجسّس على الأرض» التي أُغلقت في 2008. في 2010، راقب «مكتب القوات البحرية للتحقيق الإجرامي»⁽⁴⁸⁾ كل كومبيوتر في ولاية واشنطن يحتوي برنامجاً للشارك في الملفات بين الجمهور، سواء أكان مرتبطاً بالجيش أم لا، ما مثّل تعدياً واضحاً على القانون.

(*) نفضل استخدام تعبير «السبراني» ترجمة حرفية لـ (Cyber)، رغم إدراكنا ثقلها وعدم شيوعها، تمييزاً لها عن تعبير الإلكتروني أو الافتراضي أو الشبكي، التي تتقاطع معها أحياناً من حيث المعنى.

تجري مجموعة كبيرة من نشاطات الرقابة على البيانات والمعلومات، خارج أطر الحكومة الفيدرالية الأميركية. فمنذ 11/9، أنشأت الولايات المتحدة «مراكز انصهار» ونشرتها في أرجاء البلاد⁽⁴⁹⁾. وبوجه عام، تدار تلك المراكز من قِبل السلطات المحلية في كل ولاية، بالتعاون مع قوى الشرطة فيها. وقُصد من المراكز أن تكون جسراً للمعلومات بين تلك السلطات المحلية والوكالات القومية كالـ «إف بي آي» و«وزارة الأمن القومي». وتمنح المراكز للشرطة المحلية حق وصول لم يكن متاحاً لها من قبل⁽⁵⁰⁾ إلى بيانات الرقابة وقدراتها، وافترض أساساً أنها سوف تركز على الإرهاب⁽⁵¹⁾، لكنها استعملت لدعم إنفاذ القانون على نطاق يتوسع باطراد. ولأنها تدار محلياً، تتفاوت القوانين التي تتبعها بين مركز وآخر، كما يتفاوت مستوى الالتزام بالقوانين أيضاً. هنالك قليل من الإشراف القانوني⁽⁵²⁾، وربما بعض التدخل غير القانوني من الجيش، وكثير من السرية. ومثلاً، يعرف عن تلك «مراكز الانصهار» أنها راقبت محتجين سياسيين⁽⁵³⁾.

تدار «الفرق المشتركة لمكافحة الإرهاب» محلياً أيضاً، وهي معروفة بطريقة ضبابية، ومحاطة بسرية فائقة⁽⁵⁴⁾. وتوزعت في التحقيق مع نشطاء سياسيين⁽⁵⁵⁾، ونشر الدعاية المضادة للإسلام⁽⁵⁶⁾، ومضايقة مدنيين أبرياء⁽⁵⁷⁾.

وبصورة إجمالية، ثمة سيل كبير من الرقابة يمارس في الولايات المتحدة، تقوده ميول إيديولوجية، وتلابسه حماسة مفرطة.

وفي الطرف الآخر من المحيط الأطلسي، تمثل «القيادة الحكومية للاتصالات» النظر البريطاني لـ «وكالة الأمن القومي». وتتخرط في عمليات تجسس واسعة على مواطنيها وعبر العالم أيضاً، انطلاقاً من مقراتها في بريطانيا، ومراكز تنصت في عُمان⁽⁵⁸⁾ وقبرص⁽⁵⁹⁾ وغيرها. وتشكل شريكاً مقرباً من «وكالة الأمن القومي»، وتمارس رقابة عامة داخل حدود بلادها وخارجها. وتشمل قائمة البلدان التي تنصت على مواطنيها ومواطني دول أخرى: ألمانيا⁽⁶⁰⁾، فرنسا⁽⁶¹⁾، الدانمارك⁽⁶²⁾،

أستراليا⁽⁶³⁾، نيوزيلندا⁽⁶⁴⁾، إسرائيل، كندا... وربما كل دولة تملك مالا كافياً كي تخصصه لأعمال الاستخبارات⁽⁶⁵⁾. وتزعم الحكومة الأسترالية أن رقابتها في أندونيسيا ساعدت في إجهاض هجمات إرهابية في ذلك البلد⁽⁶⁶⁾.

نعرف قليلاً جداً عن الرقابة الحكومية في بلدان أخرى، لكننا لا نفترض أن أموراً مشابهة لا تحدث هناك، لمجرد عدم وجود من يدق النفير ويلقي ضوءاً كاشفاً عليها. تنهض الحكومات الأخرى بأشياء مماثلة حيال الإنترنت، ووفق ما تستطيع أن تضع يدها عليه، مع وجود قيود قانونية أقل على نشاطات تلك الحكومات في الرقابة.

إذ إن روسيا تجمع وتخزن وتحلل البيانات عن المكالمات الهاتفية⁽⁶⁷⁾، ال «إيميل»، استخدام الإنترنت، شبكات التواصل الاجتماعي، معاملات البطاقات الائتمانية وغيرها. وأنشأت «نظام التحقيقات والإجراءات العملانية»، ويعرف باسمه المختصر «سورم» (SORM)، استناداً إلى البنية الروسية على الإنترنت⁽⁶⁸⁾. ورأينا لمحات عن المدى الواسع لعمل «سورم» أثناء دورة الألعاب الشتوية في «سوتشي» 2014⁽⁶⁹⁾. وحينها، تمكنت السلطات الروسية من رقابة معظم ما يجري على خطوط الإنترنت في بلدها. أعطى الإرهاب والجريمة ذرائع للرقابة، لكنها تصل إلى معلومات تستعمل ضد الروس من صحافيين ونشطاء حقوق الإنسان ومعارضين سياسيين⁽⁷⁰⁾.

تحاول الصين أيضاً ترصد كل أفعال مواطنيها على الإنترنت⁽⁷¹⁾، وبدرجة أكبر خارج تلك الشبكة أيضاً. وتستخدم الصين أيضاً «المعلومات المكانية» من الهواتف الخلوية كي تتعقب الناس جماعياً⁽⁷²⁾. وتخرق الخلويات عن بُعد كي تنتصت على الناس⁽⁷³⁾، كما تراقب الأمكنة العامة بواسطة ما يتراوح بين 20 مليون و30 مليون كاميرا للرقابة⁽⁷⁴⁾. وعلى غرار روسيا، تشكل الجريمة التبرير المعلن لذلك التجسس كله، لكن الانشقاق يمثل حجة كبرى أيضاً. ويمثل «توم-سكايب» (TOM-Skype) نظاماً لخدمات التراسل بالفيديو والرسائل النصية، وهو مبادرة

مشتركة بين «مايكروسوفت» وشركة «توم أون لاين» الصينية. إن الرسائل التي تحتوي كلمات⁽⁷⁵⁾، كـ «تيانانمن» و«منظمة العفو الدولية» و«هيومن رايتس ووتش» (Human Rights Watch) [«المنظمة الدولية لحقوق الإنسان»]، وكذلك الإشارات إلى المخدرات والأفلام الإباحية الجنسية، تنسخ وتخزن كلها. ويعمل ما يزيد على 30 ألف رجل شرطة في رقابة الإنترنت⁽⁷⁶⁾.

قبل بضع سنوات، مرّت أمام أعيننا لمحات من الرقابة العالمية على الإنترنت، عندما هدّدت الهند⁽⁷⁷⁾، وروسيا⁽⁷⁸⁾، والسعودية⁽⁷⁹⁾، وأندونيسيا⁽⁸⁰⁾، ودولة الإمارات العربية المتحدة⁽⁸¹⁾، بحظر شركة «بلاك بيري» (Black Berry) ما لم تسمح لتلك الدول بالدخول إلى البيانات عن اتصالات المستخدمين. عقدت «بلاك بيري» اتفاقية مع الهند⁽⁸²⁾، احتفظت الشركة بموجبه بأمن بيانات مستخدمي تلك الهواتف، مقابل حق الحكومة في الوصول في حالات فردية إلى البريد الإلكتروني للمستخدمين، ومحادثاتهم الإلكترونية، والمواقع التي يدخلونها على الإنترنت. لا نعرف ما هي الصفقات التي أبرمت مع بقية الدول، لكن من المستطاع أن نفترض أنها سارت على نحو مماثل.

وغالباً، تلجأ الدول الصغيرة إلى الكبيرة للحصول على مساعدتها في بناء بنيتها التحتية للرقابة. حصلت إيران على مساعدة الصين في بناء رقابة مندمجة مع بنية الإنترنت فيها⁽⁸³⁾. وسأستفيض في الفصل 6 في الحديث عن الشركات الغربية التي تساعد حكومات قمعية في بناء نُظم للرقابة.

إن الأفعال التي تأتينا تلك البلدان وغيرها - أستطيع وضع كتاب مملوء بالأمثلة عنها - هي أشد قمعاً وتوتاليترية من الولايات المتحدة وحلفائها كافة⁽⁸⁴⁾. وتفرض الولايات المتحدة تحديدات وقيوداً قانونية على عمليات جمع المعلومات من قبل الحكومة⁽⁸⁵⁾، ما يفوق بكثير الدول الأخرى على الكرة الأرضية، بما فيها الاتحاد الأوروبي. في الهند⁽⁸⁶⁾ وتايلاند⁽⁸⁷⁾ وماليزيا⁽⁸⁸⁾، يمثل اعتقال الناس بأثر

من محادثات شبكية ونشاطات على الإنترنت عُرفاً سائداً. سأحدث عن المخاطر والأضرار في الفصل 7، أما الآن، فسوف أقصّر حديثي على القدرات.

الحكومة بوصفها «هاكر»

هناك فارق هائل بين التجسّس الإلكتروني كما كانه إبان «الحرب الباردة»، وحاله حاضراً. قبل عصر الإنترنت، عندما كانت الرقابة تتكوّن أساساً من تجسّس الحكومات على بعضها بعضاً، يجب على مؤسّسات كـ «وكالة الأمن القومي» أن تستهدف دارات إلكترونية محدّدة، كأن تكون كابلاً بحرياً للاتّصالات يربط بين مدينتي «برويفلوفسك» و«فلاديفستوك»، قمراً اصطناعياً للاتّصالات، وشبكة لربط الهواتف بنظام الموجات الفائقة الصغر («ميكروويف»). وفي معظم الأحيان، كان ذلك النشاط سلبياً ولا يستلزم سوى زرع رادارات كبيرة في دول مجاورة.

في المقابل، تعتمد الرقابة الحديثة على الانخراط بفعاليّة في اختراق شبكات الكمبيوتر عند العدو، وزرع برامج خبيثة مصمّمة كي تسيطر على تلك الشبكات و«ترشيح الملفات إلى خارجها»، وفق تعبير تستخدمه «وكالة الأمن القومي» لوصف سطوها على الملفات. ويقول أشد صراحة، لم تعد الطريقة الأسهل للتجسّس على اتّصالاتك هي اعتراضها أثناء نقلها بالشبكات، بل اختراق كومبيوترك والدخول إليه.

وتجري الحكومات مجموعات ضخمة من عمليات اختراق الحواسيب.

في 2011، استطاع «هاكر» إيراني أن يخترق نظام الكمبيوتر في سلطة المصادقة الإلكترونية في الدانمارك⁽⁸⁹⁾، واسمها «ديجينوتار» (DigiNotar). وبفضل ذلك، استطاع ذلك الـ «هاكر» أن يتحلل هويّة كيانات إلكترونيّة كبرى تدخل إلى الإنترنت في الدانمارك بعد حصولها على مصادقة من «ديجينوتار». وبذا، انتحل هويّة مؤسّسات كـ «غوغل» و«سي آي إيه» و«أم آي 6» و«موساد» و«مايكروسوفت» و«ياهو»

و«سكايب» و«فيسبوك» و«تويتر» و«خدمة تحديث نظام ويندوز» وغيرها. وبذا، بات متاحاً له أن يتجسس على مستخدمي تلك الخدمات. وكذلك درّب آخرين على تلك القدرة⁽⁹⁰⁾ - تحت إشراف شبه مؤكد من الحكومة الإيرانية - الذين استعملوا تلك الطريقة في الرقابة الجماعية لإيرانيين، بل ربما لأجانب أيضاً. وحينها، قدّرت شركة «فوكس - آي تي» (Fox-IT) أنه جرى اختراق 300 ألف حساب إيراني على بريد «جي ميل» الإلكتروني⁽⁹¹⁾.

في 2009، عثر بحّاث كنديون على جزء من برنامج خبيث اسمه «غوست نت» (GhostNet)⁽⁹²⁾، في كومبيوترات الدالاي لاما، المعارض للحكومة الصينية. ومثل «غوست نت» برنامجاً متطوراً لشبكة رقابة يديرها كومبيوتر في الصين. ومع التعمق في البحث، عثر على ذلك البرنامج عينه في كومبيوترات مؤسسات سياسية واقتصادية وإعلامية، موجودة في 103 بلدان. باختصار، كانت تلك قائمة الأهداف الأكثر تفضيلاً لدى الاستخبارات الصينية. ويمثل برنامج «فلايم» (Flame) أداة للرقابة الإلكترونية⁽⁹³⁾، وعثر عليه الباحثون في الشبكات الإيرانية في 2012؛ ونعتقد بأن إسرائيل والولايات المتحدة زرعته هناك وفي أماكن أخرى. واستمر برنامج «ريد أكتوبر» (RedOctober)⁽⁹⁴⁾ في التجسس بخفاء على الكومبيوترات في العالم، إلى أن عثر عليه في العام 2013، ويعتقد بأنه يمثل نظاماً روسياً للرقابة. ويشبهه فيروس «تورلا» (Turla) الذي تجسس على حكومات غربية، واكتُشف في 2014⁽⁹⁵⁾. وفي العام 2014 أيضاً، اكتُشف فيروس «ماسك» (Mask)⁽⁹⁶⁾ الذي يعتقد بأنه إسرائيلي، وهو برنامج للرقابة. واستهدف «هاكرز» إيرانيون حواسيب مسؤولين رسميين أميركيين⁽⁹⁷⁾. هنالك أكثر من ذلك بكثير من الأدوات المعروفة للرقابة الإلكترونية، ويسود اعتقاد بأن أعداداً أخرى سوف يجري اكتشافها مستقبلاً.

من باب الإنصاف، يجب القول إننا لا نملك أدلة تربط برامج الرقابة ببلدان بعينها، ولا حتى بوجود إشراف حكومي عليها. ففي معظم الأحيان، تمتنع الحكومات عن الاعتراف بأنها تخترق نظم الكومبيوتر لدى بعضها بعضاً. ومثلاً، ضمت قائمة

الأهداف في برنامج «ماسك» معظم البلدان المتحدثة بالإسبانية، ومجموعة من الكمبيوترات في المغرب وجبل طارق. ويبدو ذلك كأنه من فعل إسبانيا.

في الولايات المتحدة، كانت المجموعة التي أدمنت باختراق نُظم الكمبيوتر هي «مجموعة عمليات الدخول المنسقة» (Tailored Access Operations group) ⁽⁹⁸⁾، واشتهرت باسمها المختصر «تاو» (TAO)، وهي ضمن «وكالة الأمن القومي». نعرف أن مجموعة «تاو» تتسلل إلى الكمبيوترات عن بُعد ⁽⁹⁹⁾، مستخدمة برامج تحمل أسماء شيفرية كـ «كوانتوم إنسرت» و«فوكس أسيد». ونعرف أن «تاو» طوّرت برامج كمبيوتر مخصّصة تستطيع اختراق الأشياء الإلكترونية كافة ⁽¹⁰⁰⁾، من الكمبيوترات مروراً بمحولات الإنترنت، ووصولاً إلى الهواتف الذكية. واستطاعت «تاو» أن تحوّل بعض مكوّنات لا سلكيّة في حواسيب كثيرة، إلى «عملاء مزروعين» لها، بواسطة اعتراض إرسالها واستخدام موجاتها لدس برامج خبيثة فيها. ويشير أحد التقديرات إلى أن تلك المجموعة نجحت في اختراق 80 ألف كمبيوتر في العالم، وباتت تحصل على ملفات «ترشح» منها ⁽¹⁰¹⁾.

بديهي القول إننا صرنا نعرف عن «تاو» والجهود الأميركية في اختراق الكمبيوترات، بعد أن كشف إدوارد سنودن وثائق عالية السريّة لـ «وكالة الأمن القومي». لم تحصل تسريبات مماثلة في دول أخرى، لذا لا نعرف سوى القليل عن قدراتها في ذلك المجال.

نعرف أشياء كثيرة عن الصين ⁽¹⁰²⁾. وبموثوقيّة كبيرة، جرى تحديد الصين بوصفها مصدراً لهجمات كثيرة عالية المستوى طالت «غوغل» ⁽¹⁰³⁾ والحكومة الكنديّة ⁽¹⁰⁴⁾، وصحيفة نيويورك تايمس ⁽¹⁰⁵⁾، وشركات أميركيّة ⁽¹⁰⁶⁾ من بينها شركة «آر أس إيه» (*) (RSA) الأمنيّة ⁽¹⁰⁷⁾، والمؤسسة العسكريّة الأميركيّة ⁽¹⁰⁸⁾

(*) شركة تصنع تقنية تشفير المفتاح العام في أمن المعلومات، يتكوّن اسمها من الحروف الأولى لـ «ميتكيا»، وهم ريفست، وشامير، وأدلمان.

والمتعاقدين معها. في 2013، اكتشف بحّاث برمجيات خبيثة للحكومة الصينية في عدد من هواتف الـ «أندرويد»⁽¹⁰⁹⁾، التي يستعملها أفراد من المعارضة المناهضة باستقلال إقليم التيبّيت عن الصين. في 2014، اخترق «هاكرز» صينيّون⁽¹¹⁰⁾ قاعدة بيانات «المكتب الأميركي لإدارة الموارد البشريّة» تحتوي على معلومات عن 5 ملايين موظف حكوميّ ومتعاقد يملكون إجازات أمنيّة.

ما سبب تلك الاختراقات؟ يشكّل التجسّس السياسي والعسكري جزءاً كبيراً منها، لكن بعضها تجسّس تجاري. هناك عدد من الدول لديها تاريخ طويل من التجسّس على شركات أجنبيّة لأغراض عسكريّة وتجاريّة⁽¹¹¹⁾. تزعم الولايات المتّحدة أنها لا تمارس التجسّس التجاري، يعني ذلك أنها لا تخترق شبكات الشركات الأجنبيّة وتسطو على معلوماتها، ثم تمرّرها إلى الشركات الأميركيّة المنافسة كي تستفيد منها. لكنها تمارس التجسّس الاقتصادي⁽¹¹²⁾، باختراقها شبكات الشركات الأجنبيّة وأخذ معلومات منها كي تستخدمها الحكومة في مفاوضات تجاريّة، تستفيد منها مباشرة الشركات الأميركيّة ومصالحها. تأتي أمثلة حديثة على ذلك من شركة «بتروبراس» للنفط في البرازيل⁽¹¹³⁾، ونظام «سوفيت» الأوروبي للمعاملات البنكيّة العالميّة⁽¹¹⁴⁾. في الحقيقة، تفاخر تقرير حكوميّ أميركي صدر في 1996، بادّعاء «وكالة الأمن القومي» أنّ الصناعة الأميركيّة استفادت اقتصادياً من أحد برامجه⁽¹¹⁵⁾، «بما يصل إلى بلايين الدولارات في سنوات قليلة سابقة». ربما تكون ممن يرون أو أولئك الذين لا يرون فارقاً أساسياً بين نوعي التجسّس؛ لكن الصين التي لا يوجد فيها فارق واضح بين أعمال الحكومة والشركات، هي ممن لا يرون فارقاً بين الأمرين.

تشتري بلدان كثيرة برامج من شركات خاصة كي تستخدمها في عمليات اختراق الحواسيب. سأتحّدث بالتفصيل عن ذلك النوع من العلاقة التجاريّة في الفصل 6. وسأتناول الآن إحدى الشركات الإيطالية التي تصنع أسلحة للفضاء السبراني، واسمها «هاكينغ تيم» (Hacking Team)⁽¹¹⁶⁾، وتبيع نظماً للاختراقات

إلى حكومات عدّة كي تستخدمها الأخيرة في اختراق نُظُم التشغيل في الحواسيب والهواتف الذكيّة. ويتسلّل برنامج «هاكينغ تيم» المختص بالهواتف النّقالة إلى دواخل تلك الأجهزة، بعد أن يُرسل إليها عن بُعد، ثم يتولى جمع البريد الإلكتروني، الرسائل النصيّة، تواريخ المكالمات، دفاتر العناوين، بيانات عمليات البحث على الإنترنت، والضربات الأساسيّة على لوحة المفاتيح. وكذلك يستطيع صنع صور عن شاشة الهواتف، ورصد التراسل بين الخلوي ونظام الـ «جي بي إس». وبسرّيّة تامة، يرسل البرنامج تلك المعلومات كلها إلى الجهة التي تستخدمه. استخدمت إثيوبيا ذلك البرنامج للتسلل إلى أجهزة صحافيين أميركيين وأوروبيين⁽¹¹⁷⁾.

لعلّه من المنطقي الافتراض أن معظم الحكومات تمتلك قدرات على الاختراق الإلكتروني. أما مسائل من نوع ضد من تستخدم تلك القدرات، وما هي القيود القانونيّة للسيطرة عليها، فتلك أمور تتفاوت بين دولة وأخرى.

الهجمات الحكوميّة

عندما تلقينا التقارير الأولى عن اختراق صينيّين للشبكات الأميركيّة بهدف التجسس، شجبنا ذلك الأمر بلغة قاسية. وصنّفنا الأفعال الصينيّة⁽¹¹⁸⁾، كـ «هجمات سبرانية»، وأحياناً رمينّاها بمصطلح «حرب سبرانية»⁽¹¹⁹⁾. وبعد أن كشف سنودن أن «وكالة الأمن القومي» كانت تفعل تماماً ما يقوم به الصينيون، على مستوى العالم بأسره، استخدمت الولايات المتّحدة عبارات ملطفة كثيراً في وصف أفعالها⁽¹²⁰⁾، مستخدمة مصطلحات كـ «تجسس» و «جمع معلومات» أو «وضع العين»؛ مشدّدة على أنها نشاطات تتعلّق بأزمة السلم.

عندما حاولت شركة «هواوي» (Huawei) الصينيّة⁽¹²¹⁾ بيع معدّات شبكيّة إلى الولايات المتّحدة، جرى النظر إلى ذلك المسعى باعتباره «تهديداً للأمن القومي» بسبب

الخشيّة من أن تكون الحكومة الصينيّة قد دسّت «أبواباً خلفيّة»^(*) لتسريب المعلومات من تلك الشبكات إليها. ولاحقاً، عرفنا أن «وكالة الأمن القومي» تفعل الأمر نفسه⁽¹²²⁾ في معدات شركة «هواوي»، وكذلك المعدات الأميركية التي تُباع في الصين⁽¹²³⁾.

هناك مشكلة في أنّه من وجهة نظر الضحيّة، يتشابه الهجوم السبراني مع التجسّس الدولي إلى حدّ كبير⁽¹²⁴⁾. إنّ التجسّس السبراني الحديث هو أحد أشكال الهجوم السبراني⁽¹²⁵⁾، إذ يتضمّن كلاهما اختراق الشبكات في بلد آخر. ويتمثّل الفارق الوحيد بينهما في تعمّد زعزعة الشبكات المخترقة وإثارة الاضطراب فيها، أو تجنّب ذلك الأمر. وعلى الرغم من أنّه فارق كبير، فإنه من الممكن تأخيرهِ شهوراً أو حتى سنين. ولأنّ اختراق شبكات بلد ما يؤثر في نطاقه الإقليمي، فمن شبه المؤكّد أن يكون غير شرعي بموجب قوانين ذلك البلد. وعلى الرغم من ذلك، تستمر البلدان في اختراق شبكات بعضها بعضاً.

هناك مثال على ذلك. في 2012، اخترقت «وكالة الأمن القومي» تكراراً البنية التحتية للإنترنت في سوريا. وقصّدت الوكالة من ذلك زرع برنامج شيفري للتنصّت في أحد المحوّلّات الأساسيّة لشبكة الإنترنت في ذلك البلد، لكن الوكالة تسبّبت عرضاً في انقطاع الإنترنت عن البلد بأكمله⁽¹²⁶⁾. إنّ ضرب شبكة الإنترنت في بلد ما أو محاولة استخراج ملفات منها، هما أمران يجريان بواسطة العمليات نفسها بالضبط.

تعيش الحكومات الزمن الكبير للحرب السبرانيّة في الفضاء الافتراضي. وتمتلك 30 بلداً قواتٍ للحرب السبرانيّة في جيوشها⁽¹²⁷⁾، هي: الولايات المتّحدة، روسيا، الصين، معظم بلدان الاتحاد الأوروبي، إسرائيل، الهند، البرازيل، أستراليا، نيوزيلندا، ومجموعة من البلدان الأفريقيّة. في الولايات المتّحدة، يقود تلك القوّات «المركز الأميركي لقيادة الحرب السبرانيّة» في وزارة الدفاع. ويتولّى الأميرال مايكل

(*) هي مناطق في الشيفرة الإلكترونيّة للبرامج يجري توهينها عمداً، لتسهيل التعرّف إلى منظومتها واختراقها، ثم الدخول منها إلى بقية الشيفرة.

إس. روجرز قيادة القوّات السبرانيّة و«وكالة الأمن القومي» معاً. ويظهر ذلك مدى تقارب المهمتين.

ثمة أمثلة قليلة معروفة عن قدرة الهجمات السبرانيّة في التسبّب بأذى فعليّ في الأرواح أو الممتلكات. في 2007، وقعت أستونيا ضحية لسلسلة واسعة من الهجمات السبرانيّة⁽¹²⁸⁾. غالباً ما يشار إلى ذلك باسم «الحرب السبرانيّة الأولى»؛ نظراً لترافقه حينها مع تصاعد التوتر بين أستونيا وجارتها روسيا. وقعت جورجيا، وهي جمهوريّة سوفياتيّة سابقة، ضحية لسلسلة من الهجمات السبرانيّة التي سبقت بعام غزواً بريّاً للقوات الروسيّة⁽¹²⁹⁾. في 2009، كانت كوريا الجنوبيّة ضحية هجمات سبرانيّة⁽¹³⁰⁾. وشُنّت تلك الهجمات كلها بأسلوب «منع الخدمة»، الذي يركّز إلى ضخّ كميات ضخمة من المواد والملفات الرقميّة إلى المواقع المستهدفة، إلى حدّ «إتخامها» وشل قدرتها على العمل بصورة مؤقتة. إنّها ضربات مثيرة للاضطراب، لكنها لا تحدث أذى عميق الغور، على المدى الطويل.

في تلك الهجمات عينها أيضاً، لم تتوافر أدلة مؤكّدة على هويّة المعتدي، ولا حتى إذا كان جهة حكوميّة أم لا. في 2009، نُسبَت الهجمات على أستونيا إلى مجموعة شبابيّة مؤيدة للكرملين⁽¹³¹⁾، على الرغم من أنّه لم يُدّن أحد رسمياً سوى شاب روسي عمره 22 سنة⁽¹³²⁾، من سكان مدينة «تالين»، عاصمة أستونيا. ويندر الوصول إلى ذلك المستوى من التعرّف إلى هويّة منفّذي الهجمات السبرانيّة. وعلى غرار هجمات التجسّس التي نوقشت قبلاً، يصعب تتبع الهجمات السبرانيّة. ويتركّ لنا أن نحُدّس بهوية المعتدي استناداً إلى قائمة الضحايا. في حال وجود توترات إثنية مع روسيا، تنسب الهجمات إلى روسيا بالطبع. إذا هوجمت كوريا الجنوبيّة، فمن غير كوريا الشماليّة قد تحرّك لمهاجتها؟

يعرّف الفيروس الإلكتروني «ستاكس نت» (Stuxnet) بوصفه أول سلاح سبراني بمستوى عسكري⁽¹³³⁾. أطلق في 2009 من قبل الولايات المتّحدة

وإسرائيل كي يضرب منشأة «نطنز» النووية في إيران، ونجح في إحداث أضرار مادية مباشرة⁽¹³⁴⁾. وشهد العام 2012، هجمة سبرانية استهدفت منشأة «آرامكو» السعودية، في ما يعتقد بأنه رد إيراني⁽¹³⁵⁾.

شبكة مفردة للرقابة الدولية الشاملة

هنالك قوة دفع نحو الاحتكار تتولد من الرقابة الإلكترونية الشاملة. في مطلع هذا الفصل، تحدثت عن الفارق بين تجسّس الحكومات على بعضها بعضاً، والرقابة الحكومية على الشعب. وبشكل أساسي، يسير التجسّس الحكومي وفق خطوط السياسة، وتنازّر بلدان متحالفة في التجسّس على أعدائها. وفعلنا ذلك أثناء «الحرب الباردة». إنها السياسة.

تمثّل الرقابة الشاملة أمراً مختلفاً. إذا كنت قلقاً حقاً من إمكان أن تأتيك هجمات من أي شخص وأي مكان، تشعر بالحاجة إلى التجسّس على كل شخص في كل مكان. ولأن لا بلد يستطيع فعل ذلك وحده، يبدو منطقياً التشارك في المعلومات مع بلدان أخرى⁽¹³⁶⁾.

لكن، مع من تشارك في معلوماتك وبياناتك؟ بإمكانك أن تشارك مع حلفائك عسكرياً، لكنهم ربما لا يتجسّسون على بلدان تهتم أنت بها. وربما كانت مستوى رقابتهم لكوكب الأرض وسكانه، لا تلبي هواجسك بشكل كافٍ، فلا تبدو مشاركتك إياهم المعلومات أمراً مجدياً. يكون من الأفضل منطقياً أن تشارك⁽¹³⁷⁾ مع دولة تملك شبكة التجسّس الأكثر اتساعاً في العالم: الولايات المتحدة.

تصف تلك الكلمات ما يجري حاضراً. إذ تشارك الاستخبارات الأميركية مع بلدان عدّة. هناك تشارك بين بلدان صديقة لبعضها بعضاً، وتتمتع بالثروة وتتكلم الإنكليزية، وتسمّى «العيون الخمس» (Five Eyes)⁽¹³⁸⁾: الولايات المتحدة، المملكة المتحدة، كندا، أستراليا، ونيوزيلندا. وتضم شراكة «العيون التسع»⁽¹³⁹⁾ البلدان

الخمسة السابقة، إضافة إلى فرنسا، والدانمارك، وهولندا، والنرويج. وتشمل شراكة الـ «14 عيناً»⁽¹⁴⁰⁾ البلدان التسعة السابقة، إضافة إلى ألمانيا، وبلجيكا، وإسبانيا، وإيطاليا، والسويد⁽¹⁴¹⁾. وتشارك الولايات المتحدة مع بلدان محافظة تقليدياً كاهند وباكستان، إضافة إلى نُظم قمعية أخرى (...)⁽¹⁴²⁾.

تعطي تلك البلدان كلها لـ «وكالة الأمن القومي» الحق في الوصول إلى كل شيء تقريباً⁽¹⁴³⁾. في شهادة تقدّم بها إلى الاتحاد الأوروبي في 2014، أورد سنودن أنه «بالنتيجة، هناك «بازار» أوروبي ربما يقدم فيه بلد عضو في الاتحاد الأوروبي كالدانمارك، إلى «وكالة الأمن القومي» الحق في الوصول إلى كل شيء مع وضع شرط (غير ملزم) بعدم رقابة الدانماركيين؛ كما قد تعطي ألمانيا حقاً مشابهاً إلى «وكالة الأمن القومي» شرط عدم رقابة الألمان. ولكن، من الممكن أن يكون مركزا اختراق الإنترنت (أحدهما بمشاركة ألمانيا والآخر الدانمارك)، عبارة عن نقطتين على الكابل نفسه. وبذا، تحصل «وكالة الأمن القومي» على معلومات عن المواطنين الألمان عندما تمرّ حركتهم على الإنترنت بالدانمارك، وتحصل على معلومات عن المواطنين الدانماركيين عند مرور حركتهم على الإنترنت بألمانيا؛ فيما يعدّ ذلك كله متوافقاً تماماً مع الاتفاقيات الموقعة مع البلدين».

في العام 2014، صرنا نعرف أن «وكالة الأمن القومي» تتجسّس على الحكومة التركية، فيما تشارك في الوقت عينه مع تركيا للتجسّس على المتمرّدين الأكراد في تركيا⁽¹⁴⁴⁾. وكذلك علمنا أن «وكالة الأمن القومي» تتجسّس على أحد أكثر شركاء الرقابة قرباً منها: ألمانيا⁽¹⁴⁵⁾. ويسود اعتقاد بأننا نتجسّس على شركائنا جميعهم⁽¹⁴⁶⁾، فيما عدا الشركاء الأربعة في «العيون الخمس». وحتى عندما تتفاخر «وكالة الأمن القومي» بنجاحاتها في مكافحة الإرهاب⁽¹⁴⁷⁾، يكون معظمها تهديدات أجنبية كانت موجهة ضد بلدان أجنبية، بمعنى أنها لا تتعلّق بالولايات المتحدة.

ليس أمراً مفاجئاً القول إن الولايات المتحدة تتشارك المعلومات مع إسرائيل. وتقليدياً، تزال أسماء الأميركيين قبل المشاركة في المعلومات بين الولايات المتحدة وبلدان أخرى، بهدف حماية أمن الأميركيين. لكن، يبدو أن إسرائيل تمثل استثناءً. إذ تعطي «وكالة الأمن القومي» إسرائيل «الوحدة 8200» السرية التي تتضمن «سيغينت الخام» (raw SIGINT)⁽¹⁴⁸⁾، وهي النظام السري للإشارات في الاستخبارات الأميركية.

حتى الأعداء التاريخيون لأميركا يتشاركون المعلومات والبيانات معها، ولو أن ذلك يجري ضمن نطاق ضيق⁽¹⁴⁹⁾. بعد هجمات 9/11، أعادت روسيا تصنيف الانفصاليين الشيشان بوصفهم إرهابيين، وأقنعت الولايات المتحدة بأنها تقدم مساعدة بالتشارك في المعلومات⁽¹⁵⁰⁾. في 2011، حذرت روسيا الولايات المتحدة من تاملان تسارنايف، مفجّر سباق ماراثون بوسطن⁽¹⁵¹⁾. وردّت الولايات المتحدة الجميل بفرض رقابة على التهديدات في «دورة سوتشي الأولمبية»⁽¹⁵²⁾.

لا تبدو تلك المشاركات منطقية إذا نظر إليها من زاوية تجسّس الحكومات على بعضها بعضاً، لكنها تغدو واضحة وملائمة عندما يكون هدفها الرئيس هو الرقابة العامة. وبذا، ففيما تعلن ألمانيا غضبها من تجسّس «وكالة الأمن القومي» على قادتها، يستمر جهازها للاستخبارات «بي آن دي» (BND) في التعاون مع «وكالة الأمن القومي» لرقابة الآخرين جميعهم.

ليست محصلة تلك الأمور كلها سارة أبداً، بل تتمثل في نسج شبكة عالمية شاملة، تتواطأ فيها الدول لرقابة كل شخص على الكرة الأرضية. ربما تأخرت تلك الشبكة في الظهور لفترة ما، فهناك بلدان ما زالت خارجها كروسيا التي تصرّ على فعل كل شيء بنفسها، وكذلك تحول الخلافات الأيديولوجية الصلبة دون أن تتعاون دولة كإيران مع روسيا أو الولايات المتحدة؛ لكن معظم البلدان الصغيرة ستجد أسباباً للانخراط في تلك الشبكة. ومن وجهة نظر ضيقة تماماً، ربما كان ذلك هو الشيء المنطقي الذي يجب القيام به.

6

تعزير السيطرة المؤسسية

لا تنفصل رقابة الحكومة عن نظيرتها لدى الشركات. إنها متشابكتان في نسيج واحد، وتعتمد إحدهما على الأخرى. إنها شراكة القطاعين العام والخاص التي تطوف بالعالم. إنها ليست اتفاقية رسمية، بل تحالف مصالح⁽¹⁾. وعلى الرغم من أنها ليست مطلقة، فإنها صارت حقيقة مسلماً بها، مع سعي لاعبين أقوياء من المسكين بالمصالح فيها إلى جعلها تستمر إلى الأبد. وعلى الرغم من أن وثائق سنودن عن رقابة «وكالة الأمن القومي» أحدثت شروخات في تلك الشراكة، وهو أمر سأتناوله في الفصل 14، فإنها ما زالت قوية.

أوضحت وثائق سنودن مدى اعتماد «وكالة الأمن القومي» على الشركات الأميركية في التجسس على الإنترنت. إذ لم تبين «وكالة الأمن القومي» نظام التنصت على الإنترنت من لا شيء. لاحظت الوكالة أن عالم الشركات أنجز بناء ذلك النظام، فاخترته واعتمدت عليه. وبواسطة برامج كـ «بريزم» (PRISM)، أرغمت «وكالة الأمن القومي» شركات كـ «مايكروسوفت» و«غوغل» و«آبل» و«ياهو»، على إمدادها ببيانات عن بضع آلاف من الأشخاص الذين اهتمت بهم الوكالة. وبواسطة برامج أخرى، حصلت «وكالة الأمن القومي» على نفاذ مباشر إلى التركيب الأساسي للإنترنت⁽²⁾؛ كي تمارس رقابة واسعة شملت الجميع. وأحياناً، تعاونت تلك الشركات مع الوكالة طوعاً. وفي أحيان أخرى، أرغمتها المحاكم على

تسليم البيانات والمعلومات، غالباً بطريقة سرية. في أحيان أخرى، اخترقت الوكالة البنية التحتية الإلكترونية للشركات، من دون الحصول على إذن من الأخيرة.

يحدث ذلك في العالم بأجمعه. إذ تستخدم دول عدة قدرات الرقابة لدى الشركات كي تراقب مواطنيها. وبواسطة برنامج كـ «تيمبورا» (TEMPORA) تدفع «القيادة الحكومية للاتصالات» في المملكة المتحدة، إلى شركات اتصالات كـ «بي تي» (BT) و«فودافون» (Vodafone) ⁽³⁾؛ كي تعطيها منافذ إلى الكتل الرئيسة للاتصالات في العالم بأكمله. وتقدم «فودافون» إلى حكومات ألبانيا، ومصر، وهنغاريا، وإيرلندا، وقطر (وربما ما مجموعه 29 بلداً)، منافذ للدخول مباشرة إلى حركة الإنترنت في بلدانها ⁽⁴⁾. ولا نعرف إلى أي مدى تدفع تلك الحكومات لقاء منافذ الدخول على الاتصالات والإنترنت، كما تفعل المملكة المتحدة أيضاً، أم إنها تحصل عليها بمجرد طلبها. وتنصت الحكومة الفرنسية على «فرانس تليكوم» (France Télécome) و«أورانج» (Orange) ⁽⁵⁾. سبق أن تحدثنا عن الصين وروسيا في الفصل 5. تحوز عشرات البلدان قوانين عن الاحتفاظ بالمعلومات ⁽⁶⁾ - أعلن الاتحاد الأوروبي أنها تعدّ غير دستورية في 2014 - تفرض على مقدمي خدمة الإنترنت الاحتفاظ بالبيانات المتعلقة بزبائنهم بضعة شهور، كي تراجعها الحكومة في حال رغبت بذلك. ويجب على مقاهي الإنترنت في إيران ⁽⁷⁾، وفيتنام ⁽⁸⁾، والهند ⁽⁹⁾، وغيرها، الحصول على معلومات عن هويات مستخدميها والاحتفاظ بها.

تحدث أشياء مماثلة خارج الإنترنت. ومباشرة عقب 9/11، اشترت الحكومة الأمريكية بيانات من سيطرة المعلومات ⁽¹⁰⁾، شملت الحصول على بيانات المسافرين جواً من شركة «تورش كونسبتس» (Torch Concepts) ⁽¹¹⁾، وقاعدة بيانات الناهخين المكسيكيين من شركة «تشويس بوينت» (ChoicePoint) ⁽¹²⁾. يفرض القانون الأمريكي على المؤسسات المالية تقديم تقارير للحكومة عن المعاملات النقدية التي تزيد قيمتها على عشرة آلاف دولار ⁽¹³⁾، وينخفض الرقم إلى ألف دولار في حال صرف عملات أجنبية. تفرض مجموعة من الحكومات على الفنادق الإبلاغ عن

الأجانب الذين يقضون ليلة فيها، فيما تفرض مجموعة أكبر من الأولى على الفنادق الحصول على نسخ من بطاقات الهوية وجوازات السفر للنزلاء الأجانب. وكذلك تستعمل كثير من الحكومات كاميرات الرقابة في الأماكن العامة، ونُظم تصوير لوحات المركبات، و«البيانات المكانية» للخلوي.

وفي السياق عينه، تحصل الشركات على معلومات حكومية وتستعملها لمصلحتها. إذ تباع ولايات كاليفورنيا⁽¹⁴⁾ وأوهايو⁽¹⁵⁾ وتكساس⁽¹⁶⁾ وفلوريدا⁽¹⁷⁾، بيانات عن رخص قيادة المركبات تشمل الصور، إلى شُرّة من القطاع الخاص. تباع ولايات أخرى بيانات تسجيل الناخبين⁽¹⁸⁾. في 2014، اقترحت الحكومة البريطانية بيع بياناتها عن ضرائب الدخل⁽¹⁹⁾، لكن احتجاجاً عمومياً أدى إلى تأجيل تلك الخطوة، مؤقتاً على الأقل. وتزعم «الخدمات الصحية الوطنية» في المملكة المتحدة، بيع البيانات الصحية للمرضى إلى شركات الأدوية والتأمين الصحي⁽²⁰⁾. ثمة حلقة من التغذية الراجعة⁽²¹⁾: تناقش الشركات لمصلحة الحق في الحصول على المعلومات من الحكومة، ثم تحتاج بأن تلك المعلومات يجب أن توضع تحت قوانين حكومية مفتوحة، وبعد ذلك؛ تطلب الشركات المعلومات كي تبيعها إلى الحكومة مجدداً.

وتكون النتيجة النهائية تداول كميات كبيرة من بيانات الرقابة ومعلوماتها بين الشركات والحكومات. وكذلك تكون إحدى النتائج المباشرة لتلك العملية صعوبة تمرير قوانين فعالة للجم رقابة الشركات؛ ذلك أن الحكومات لا ترغب فعلياً في تقييد حصولها هي نفسها على البيانات والمعلومات بلجم ممارسة الشركات للرقابة، طالما أن الأخيرة تمدّ الحكومات ببيانات عنها.

يصلح النقاش عن شعار «لا تتعقب» نموذجاً قوياً عن رداءة الوضع حاضراً. فلسنوات طويلة، حاول نشطاء الدفاع عن الخصوصية تمرير قانون يفرض أن يُعطى مستخدمو الإنترنت خياراً يمكنهم من تهئية محرّكات البحث بما يحول دون تتبعهم من قبل المواقع التي يزورونها على الإنترنت⁽²²⁾. اقترحت مجموعة كبيرة

من القوانين الوطنية في الولايات المتحدة عن ذلك الأمر، لكن شركات الإنترنت قاومتها بضراوة، ولم يمرر أي قانون في ذلك الشأن. وفي 2013، مرّرت ولاية كاليفورنيا قانوناً من ذلك النوع، لكن مجموعات الضغط خفّفته مراراً وتكراراً حتى باتت منفعة مستخدمي الإنترنت منه ضئيلة للغاية. ووفق ذلك القانون، تملك الحق كمستخدم في إبلاغ المواقع بأنك ترغب في ألا تلاحق على الإنترنت، ولكن المواقع تملك الحق أيضاً في تجاهل رغباتك.

تختلف الأمور قليلاً في أوروبا⁽²³⁾. هناك قانون كـ «التوجيه بشأن حماية البيانات»، يفرض قيوداً أكبر على رقابة الشركات، وقد أحدث بعض التأثير. في المقابل، جرى التوقيع على «معاهدة الملاذ الآمن»^(*) بين الولايات المتحدة والاتحاد الأوروبي، وهي تعني أن البيانات والمعلومات الشخصية يمكنها أن تتدفق من الاتحاد الأوروبي إلى شركات المعلوماتية الأميركية في الولايات المتحدة⁽²⁴⁾، التي تفرض قيوداً أقل تشدداً من تلك التي يطبقها الاتحاد الأوروبي.

شراكة القطاعين العام والخاص في الرقابة⁽²⁵⁾

لا تمارس الحكومات الرقابة والحجب والتحكّم بالعمليات على الشبكات بواسطة أجهزتها وحدها؛ إذ تلقى دعماً من شراكة واسعة في الرقابة بين القطاعين العام والخاص، يتمثل في مروحة من الشركات الساعية للربح. في 2010، بيّن تحقيق أن 1931 شركة مختلفة داخل الولايات المتحدة تعمل في الاستخبارات ومكافحة الإرهاب وأمن الوطن⁽²⁶⁾. وفي مقال ظهر عام 2013، أوردت صحيفة واشنطن بوست أن 70 ٪ من ميزانية الاستخبارات في الولايات المتحدة تذهب إلى شركات خاصة⁽²⁷⁾، وأن 483 ألف متعاقد مع الحكومة يملكون تراخيص سرية جداً، وهم ثلث عدد أصله 1.4 مليون متعاقد مع الاستخبارات. في ذلك، تبرز

(*) عند ترجمة الكتاب، كانت معاهدة لم يكشف الطرفان تفاصيلها، اسم "برايفسي شيلد" (Privacy Shield)، حلتّ بديلاً لهذه المعاهدة التي ألغتها «محكمة العدل الأوروبية» أواخر 2015.

بوضوح سياسة «الباب الدوّار» في العلاقة بين الحكومة والشركات المتعاقدة معها في الاستخبارات.

غادر الأميرال مايك ماكّونيل «وكالة الأمن القومي» بعد أن ترأسها بين عامي 1992 و 1996، ليصبح نائباً لرئيس شركة «بوز آلن هاملتون»^(*) (Booz Allen Hamilton) مستمراً في العمل على مسائل تتعلق بالأمن القومي.

وبعد أن تقاعد من إدارة «وكالة الأمن القومي» في 2013، أنشأ كيث ألكسندر شركة مختصة بالاستشارات عن أمن الإنترنت⁽²⁸⁾، وحصل على براءات اختراع عن تقنيات في الأمن زعم أنها طوّرت زمن ولايته. ووظّف في شركته المدير الرئيسي للتكنولوجيا في «وكالة الأمن القومي» مع استمرار الأخير في العمل ضمن الوكالة⁽²⁹⁾.

تبيع مجموعة من الشركات الصانعة للأسلحة السبرائية أدوات لاختراق الشبكات إلى حكومات عدّة. ومثلاً، يوصف برنامج «فِن فيشر» (Fin Fisher)⁽³⁰⁾ من قبل شركته الصانعة «غاما غروب» (Gamma Group) الألمانية-البريطانية، بأنه «حلّ معلوماتي هجومي للاقتحام». وتشترى حكومات عدّة ذلك البرنامج كي تتجسّس على حواسيب الناس وهواتفهم الذكية. في 2012، عثر بحّاث على أدلة عن استخدام «فِن فيشر»⁽³¹⁾ في البحرين وسنغافورة وأندونيسيا ومنغوليا وتركمانستان ودولة الإمارات العربية المتحدة وإثيوبيا وبروناي، إضافة إلى الولايات المتحدة وهولندا.

في الفصل 5، تناولت المجموعة الإيطالية «هاكينغ تيم». وتستعمل أدواتها الرقمية المخصصة لاختراق الكمبيوتر والخلوي الذكي ومتجاتها الإلكترونية للرقابة من قبل حكومات: أذربيجان وكولومبيا ومصر وإثيوبيا وهنغاريا وإيطاليا وكازاخستان وكوريا وماليزيا والمكسيك والمغرب ونيجيريا وعمان وبنا

(*) عند ترجمة الكتاب، كان اسم الشركة قد تغيّر إلى "استراتيجي أند" (Strategy &).

وبولندا والسعودية والسودان وتايلاند وتركيا ودولة الإمارات العربية المتحدة وأوزبكستان. ووظفت الحكومة المغربية⁽³²⁾ برامج «هاكينغ تيم» لاستهداف مجموعة تنشط ضمن ما يعرف باسم «صحافة المواطن» الإلكترونية وتحمل اسم «مامفاكينش»، بواسطة رسالة بريد إلكتروني زعمت أنها من مواطن مهدد بالخطر؛ لكن الملف المرفق بالـ «إيميل» كان محملاً بالبرنامج الخبيث لشركة «هاكينغ تيم».

في العام 2011، أظهرت لمتبردين اعتُقلوا في البحرين نصوص من رسائلهم في الـ «إيميل» وجلسات «الدردشة» على الإنترنت، عملت الحكومة على جمعها بواسطة أدوات رقمية حصلت عليها من شركتي «نوكيا» و«سيمنز»⁽³³⁾.

هناك أيضاً مؤتمر «عالم آي إس إس» (ISS World)⁽³⁴⁾، اختصاراً لاسم «نُظم دعم الذكاء» (Intelligence Support Systems)، الذي يدأب على إقامة معارض تجارية في مدن كدبي وبرازيليا. وفي منشوره الدعائي لمعارض العام 2014⁽³⁵⁾، أعلن الـ «آي إس إس» تخصيصه جلسات عن الرقابة المكانية، والتفتيش في سجلات المكالمات الهاتفية، والافتحام المعلومات الهجومي، وطرق كسر الشيفرة؛ فيما ضمت قائمة الشركات الراعية للمؤتمر نخبة الشركات التي تنتج تلك القدرات في الرقابة. ترسل بلدان عدّة ممثلين عنها كي يحضروا ذلك المؤتمر⁽³⁶⁾، الذي يوجد أكثر من نظير له في أوروبا والولايات المتحدة⁽³⁷⁾.

تعمل كبريات شركات الأسلحة المتعاقدة مع الجيش الأميركي⁽³⁸⁾، كـ «رايثون» (Raytheon) و«نورثروب غرومان» (Northrop Grumman) و«هاريس كوربوريشن» (Harris Corporation)، على صنع أسلحة سبرانية للجيش الأميركي. وتساعده مجموعة من كبرى شركات المعلوماتية في إنشاء مراكز للرقابة الإلكترونية في أرجاء المعمورة. وساعدت الشركة الفرنسية «بول إس إيه» (Bull SA) الحكومة الليبية في بناء مراكز للرقابة⁽³⁹⁾. واستخدمت نيجيريا شركة «إلبايت سيستمز» (Elbeit Systems) الإسرائيلية⁽⁴⁰⁾. واستعملت الحكومة السورية شركة

«سيمنز» الألمانية⁽⁴¹⁾، وشركة «إيريا إسبي إيه» (Area SpA) الإيطالية⁽⁴²⁾ وغيرهما. واشترى نظام معمر القذافي في ليبيا نظاماً للرقابة على الهواتف النقالة من شركتي «زد تي إيه» الصينية و«فاس تيك» (VASTech) الجنوب أفريقية⁽⁴³⁾. ولا نعرف من بنى نظم رقابة الإنترنت في أذربيجان⁽⁴⁴⁾ وأوزباكستان⁽⁴⁵⁾، لكن من شبه المؤكد أن شركات غربية ساعدتها في ذلك.

هنالك عدد قليل من القوانين التي تمنع نقل تقنيات الرقابة، ومعظمها يجري تغطيه بسهولة⁽⁴⁶⁾.

لا تنحصر تلك التقنيات بنظم مصممة خصيصاً للتنصت الحكومي، بل إن معظم البنية التحتية للرقابة الحكومية بُنيت كي تستخدمها الشركات⁽⁴⁷⁾. تباع الشركة الأميركية «بلو كوت» (Blue Coat) نظماً تقنية للترصد ورقابة المحتوى إلى شبكات تستعملها الشركات، كما تُستخدَم أيضاً في الرقابة الحكومية في بلدان كبورما، والصين، ومصر، وأندونيسيا، ونيجيريا، وقطر، والسعودية، وتركيا، وفنزويلا⁽⁴⁸⁾. ويستعمل برنامج تتجه شركة «نتسويبر» (Netsweeper) الكندية لرقابة المحتوى، من قبل جهات الرقابة الحكومية في قطر، واليمن، ودولة الإمارات العربية المتحدة، والصومال، وباكستان⁽⁴⁹⁾. وكذلك يستعمل برنامج رقابة المحتوى الذي تصنعه شركة «فورتينيت» (Fortinet) الأميركية، لفرض حجب على مواقع للإنترنت في بورما⁽⁵⁰⁾. وهناك برنامج مشابه اسمه «سمارت فلتر» (SmartFilter) تصنعه شركة «ماكافي» (McAfee) الأميركية، يستخدم بصورة طبيعية في المدارس، ساعد حكومات تونس وإيران في فرض حجب على مواقع الإنترنت في البلدين⁽⁵¹⁾. واستُخدمت معدات تصنعها شركة «سوفوس» (Sophos) البريطانية، لفرض رقابة على المواطنين واعتقالهم، من قبل سوريا وعدد من النظم القمعية الأخرى.

ثمة حياد في التكنولوجيا حيال القيم. إذ بإمكانك استعمال الخلوي في طلب النجدة لأناس في حالات طارئة، أو لوضع تخطيط لسرقة بنك. لا يوجد فارق

تقني بين استخدام حكومة لأداة معلوماتية في التعرف إلى مجرمين، أو استعمالها للتعرف إلى منشقين عنها. لا يوجد فوارق تقنية في استعمال حكومة لأداة معينة أو استخدامها من قبل شركة. كذلك فإن الأدوات الرقمية التي تستعملها الشركات بصورة قانونية لرقابة «إيميل» موظفيها كي لا يسربوا أسرارها، يمكن استعمالها أيضاً من قبل حكومات قمعية بهدف الرقابة والحجب. وعلى العكس من ذلك، فإن الأدوات التقنية عينها التي يستخدمها المنشقون الإيرانيون والسعوديون للتهرب من الحجب الحكومي، يمكن استعمالها أيضاً من قبل مجرمين يسعون لنشر أفلام إباحية تستغل الأطفال جنسياً. ويسمح التشفير للأشخاص الطيبين بالتواصل مع الأشرار، لكنها تسمح للشريين أيضاً بأن يتواصلوا من دون أن تنتصت عليهم الأشخاص الطيبون⁽⁵²⁾. وهناك تقنيات للتعرف إلى الوجوه تستعملها شركة «ديزني» في منتجعاتها لالتقاط صور مديريها مع الزوار كهدايا⁽⁵³⁾، ومن المستطاع استعمالها للتعرف إلى وجوه المحتجين السياسيين في الصين، ونشطاء حركة «احتلوا وول ستريت» (Occupy Wall Street) في نيويورك.

الحكومات تخرب الشبكات التجارية

حتى هذه النقطة، ناقشتُ كيف تستفيد رقابة الحكومات من القدرات التقنية للشركات. وتبدو تلك الصورة صحيحة في معظمها، ولكن لا تنأى الحكومات بنفسها أيضاً عن إرغام الشركات على التجسس لمصلحتها.

في مطالع التسعينيات من القرن الماضي، شرعت الـ «إف بي آي» في الإغراب عن قلقها من قدراتها في الرقابة على الهواتف. درجت الـ «إف بي آي» على إتمام تلك الرقابة في عصر المحوّلات القديمة للهواتف الأرضية، بجهود تتضمن غرس الملاقط في الخطوط، والتلاعب بأسلاك الخطوط، والتسجيلات على أشرطة النايلون الممغنطة. تمثّلت المشكلة حينها في أن المحوّلات الهاتفية لا تعمل بتلك الطريقة. وبدأ أن عزل رقم هاتفه بعينه أمر صعب، ما أثار قلق «إف بي آي» من

إمكان أن تفقد قدرة التنصت على المكالمات. ولذا، مارست ضغوطاً متصاعدة على الكونغرس، وحصلت في 1994، على تشريع اسمه «قانون مساعدة الاتصالات في إنفاذ القانون» (Communications Assistance for Law Enforcement Act) ⁽⁵⁴⁾، واشتهر باسمه المختصر «كاليا» (CALEA)، يفرض على شركات الاتصالات تصميم محولاتها الرقمية بما يجعل القدرة على التنصت جزءاً أساسياً مثبتاً فيها.

وبالفقر 20 سنة إلى الأمام، نرى أن الـ «إف بي آي» تريد مرة أخرى من صناعة المعلوماتية والاتصالات المتطورة أن تسهل لها مهمة الرقابة. لم يعد جزء كبير من الاتصالات يُجرى بواسطة الهاتف، بل بالتحادث في مواقع الإنترنت، والبريد الإلكتروني وموقع «سكايب». وحاضراً، تمارس الـ «إف بي آي» ضغوطاً للحصول على تحديث لقانون «كاليا» ⁽⁵⁵⁾، بما يجعله قادراً على تغطية الاتصالات المتطورة بأنواعها كافة: المكالمات الصوتية، والأشرطة والصور، والنصوص المكتوبة، وألعاب إلكترونية كـ «وورد أوف ووركراфт»، وتلك النافذة الصغيرة للردشة مع بقية المشاركين في لعبة «سكرابل» عبر الإنترنت.

يتمثل الهدف النهائي للـ «إف بي آي» في حظر الاتصالات الآمنة كافة ⁽⁵⁶⁾. ويصيح فاليري كابروني، المستشار العام للـ «إف بي آي» الأمر على النحو التالي: «يجب ألا يعد أحد المستهلكين بأنهم لن يُجلبوا إلى المحاكم الأميركية. من المستطاع وعد الناس بالحصول على تشفير قوي، لكن يجب عليهم أيضاً أن يفكروا في كيفية إيصال النص الأصلي الواضح إلى أيدينا». وتترجم تلك الكلمات بأن أحدًا لا يستطيع إمداد جمهور الزبائن باتصالات آمنة فعلياً.

واعتماداً على نوع النظام، يتدرج إنجاز ما تسعى إليه الـ «إف بي آي»، من السهل إلى المستحيل. في نُظُم كالبريد الإلكتروني «جي ميل»، يكون الأمر سهلاً. إذ تراكم الرسائل غير المشفرة في خوادم شركة «غوغل»، وتملك الشركة مكتباً بطواقم جاهزة للرد على طلبات الدخول إلى الرسائل الشخصية من حكومات في

أرجاء العالم. وتبدو برامج تشفير المحادثات من نوع «أوف ذي ريكورد» (Off the Record)، عصيّة على الاختراق، كما أنها لا تستخدم عقدة مركزية لاتصالاتها كي يجري التنصّت عليها. في تلك الحالات، يكون الحّل الوحيد لتلبية مطالب الـ«إف بي آي» هو زرع «باب خلفي» في برنامج المستخدم، ما يجعله قابلاً للاختراق من قبل الجميع. سوف أتناول مدى غباء تلك الفكرة في الفصل 11.

وعلى الرغم من الطغيان الذي يتّسم به ذلك الإجراء، فإنّ نقاشاً عاماً شرع يثور حوله، على الأقل. وغالباً، تسري هيمنة الحكومات على البنية التحتية لاتصالات الشركات، في سرية عالية، فلا نسمع بها إلا بالمصادفة.

كانت «لافابيت» (Lavabit) من الشركات التي قدّمت حماية للخصوصية أكثر مما تفعله الشركات الكبرى لخدمات البريد الإلكتروني التي يستخدمها معظمنا. وهي شركة صغيرة للبريد الإلكتروني امتلكها مبرمج اسمه لادار ليفيزون⁽⁵⁷⁾، ولقيت رواجاً بين هواة التقنيات. بلغ عدد مستخدميها نصف مليون، بينهم إدوارد سنودن.

عقب فرار سنودن إلى هونغ كونغ في 2013، تلقى ليفيزون رسالة من «وكالة الأمن القومي» تطلب الشيفرة التي تستخدمها شركة «لافابيت» في حماية مستخدميها كلّهم - مع عدم إشعارهم بإمكان أن تطالهم الرقابة⁽⁵⁸⁾. خاض ليفيزون معركة ضد تلك الرسالة في القضاء، وعندما بدا جلياً أنه بصدد الخسارة، فضّل إغلاق شركته على مخادعة زبائنه وعقد صفقة تسوية من وراء ظهورهم.

الخلاصة الأخلاقية من تلك القصة واضحة. إذا أسست عملاً تقنياً، فهناك احتمال بأن تحاول الـ«إف بي آي» أو «وكالة الأمن القومي» تحويله إلى أداة للرقابة الجماعية؛ لأنها تعتقد أن ذلك من حقّها ووفق شروطها حصرياً. تستطيع الوكالة أن ترغمك على تعديل نظامك⁽⁵⁹⁾. بإمكان الوكالة أن تفعل ذلك سرّاً، وأن ترغمك على إبقاء ذلك سرّاً. وعندما تفعل ذلك، تفقد أنت السيطرة على عملك. إذا كنت

مالكاً لشركة كبيرة، لن تستطيع إغلاقها. وواقعياً، لا تستطيع أن تنهي جزءاً من خدماتك. بطريقة واقعية تماماً، لم يعد عملك ملكاً لك. صار عملك جزءاً من الذراع القوية لأجهزة الاستخبارات الأميركية؛ وإذا تضاربت مصالحك مع مصالح الوكالة، فلسوف تكسب الأخيرة المعركة. لقد اغتُصِبَ عملك⁽⁶⁰⁾.

يتمثل السبب الوحيد لمعرفتنا تلك القصة في أن لـفيزون أدار شركته بنفسه. لم يكن لديه أسياذ على شركته، ولا مالكو مصالح فيها. كان لـفيزون قادراً على تدمير عمله بنفسه، استناداً إلى أسباب أخلاقية. لا تستطيع الشركات الأكبر حجماً، والمستحوذة من قبل كثيرين، الإقدام على ذلك. يجدر بنا افتراض أن كل شركات الكمبيوتر التي تلقت طلباً مماثلاً، خضعت في النهاية لما طُلبَ منها.

مثلاً، نعرف أن حكومة الولايات المتحدة أقنعت «سكايب» - بالرشوة والإرغام والتهديد والقهر القانوني - بإدخال تعديلات على طريقة عمل برنامجها؛ كي تسهل عمليات التنصت عليه⁽⁶¹⁾. لا نعرف ما كانت تلك التغييرات، ولا إذا ما كانت أدخلت قبل امتلاك «سكايب» من قبل «مايكروسوفت» في 2011⁽⁶²⁾، ولا حتى إذا كانت كافية بالنسبة لمطالب الحكومة، لكننا نعرف أنها حدثت⁽⁶³⁾.

في 2008، هدّدت حكومة الولايات المتحدة موقع «ياهو» سرّاً بتغريمه ربع مليون دولار يومياً، مع زيادة ذلك المبلغ يومياً، ما لم ينضمّ إلى برنامج «بريزم» (PRISM) الذي تديره «وكالة الأمن القومي»⁽⁶⁴⁾. وفي 2004، دفعت «وكالة الأمن القومي» إلى شركة «آر إس إيه» لأمن المعلومات، مقابل وضع «باب خلفي» للدخول إلى بيانات توليد الأرقام العشوائية في مكتبة نظامها للتشفير⁽⁶⁵⁾.

ثمة أنواع أخرى من استيلاء الحكومة عنوة على الأعمال، وتسري راهناً من وراء ظهر الشركات التي يجري تخريب تقنياتها في التنصت. وعندما لا تعقد «وكالة الأمن القومي» اتفاقيات مع الشركات للتنصت على نظمها، تبذل الوكالة قصارى جهدها كي يحدث ذلك بطرق خفية وملتوية. ومثلاً، عندما لم تكن راضية عن كميات

المعلومات التي تتلقاها من «غوغل» و«ياهو» بواسطة برنامج «بريزم»، اخترقت الوكالة الخطوط الرئيسة للاتصالات بين مراكز المعلومات في الشركتين⁽⁶⁶⁾، ربما بالتعاون مع الجهة التي منحتها تلك الاتصالات. وظهر رد فعل غاضب من أحد مهندسي الأمن المعلوماتي في «غوغل»⁽⁶⁷⁾، إذ كتب على صفحته الشخصية في «غوغل +»، عبارة: «ليذهب هؤلاء الناس إلى الجحيم». ومنذ ذلك الحين، لجأ «غوغل» إلى تشفير الاتصالات بين مراكز معلوماته سعياً لإبعاد الوكالة عنها. ويزعم «ياهو» أنه يفعل الأمر نفسه.

ليس ذلك مثلاً مفرداً على تعمد «وكالة الأمن القومي» اختراق شركات التكنولوجيا. إذ تصنع الوكالة صفحات مزيفة على «فيسبوك» لتخترق حواسيب الناس⁽⁶⁸⁾، ويعمل فرع «تاو» فيها على اعتراض معدات شركة «سيسكو سيستمز» أثناء عمليات الشحن؛ كي يدس مكوّناته الخاصة فيها⁽⁶⁹⁾.

لا نعرف نوع الضغط الذي تمارسه الحكومة الأميركية على المقدمين الرئيسيين للخدمة «حوسبة السحاب»، كي تقنعهم بإعطائها منفذاً إلى بيانات مستخدميها، أو إذا كانت تلك الشركات أبرمت اتفاقيات سرية مع «وكالة الأمن القومي». لكننا نعلم أن برنامجاً للوكالة اسمه «بول ران» (Bullrun) يعمل على تفكيك الشيفرات في الإنترنت، وأن نظيره البريطاني لدى «القيادة المركزية للاتصالات الحكومية» يحمل اسم «إيدج هل» (EdgeHill). ونجح البرنامجان في هزيمة معظم إجراءات أمن المعلومات الشائعة على الإنترنت. هل طلبت «وكالة الأمن القومي» من محرّك البحث «غوغل» المفاتيح الرئيسة للتشفير وأرغمته على إبقاء الأمر سراً، كما فعلت مع شركة «لافايت»؟ هل اخترقت مجموعة عمليات الدخول المنسقة في الوكالة، خوادم «غوغل» خارج أميركا ووسطت على مفاتيح التشفير فيها، أو اعترضت معدات كانت مرسلة إلى مراكز للمعلومات يملكها «غوغل» خارج أميركا، وزرعت فيها «أبواباً خلفية» لتسريب المعلومات منها؟ تمثل تلك الأمور ممارسات موثقة تنهض بها الوكالة. في الحال الأولى، يكون «غوغل» قد مُنِعَ قانونياً من الاعتراف بحدوثها؛ في الحال الثانية، لن يكون «غوغل» راغباً في الإقرار بحدوثها؛ وفي الثالثة، يكون

«غوغل» غير عارف حتى بحدوثها. بصورة عامة، نعرف أنه في السنوات التي تلت 9/11، تلقت الحكومة الأميركية سيولاً من التعاون الطوعي معها من شركات اعتقد قاداتها أن ما يفعلونه جزء من الواجب الوطني.

أعتقد بأننا سنشاهد مزيداً من الدخول إلى معظم معلوماتنا وبياناتنا، على يد «وكالة الأمن القومي»، بسبب نوع المعلومات التي تسعى إليها. إذ اعتادت الوكالة على الحصول على ما ترغب به الشركات الأساسية للإنترنت، ومقدمو خدمات الـ«برودباند» عليها.

أضحى ذلك أقل تحقّقاً لأن التشفير - خصوصاً النوع المسمّى تشفير الـ«إس إس آل» (SSL) - بات أكثر انتشاراً. ويصبح أقل تحقّقاً كلما زادت عمليات التشفير على الإنترنت. للتغلب على ذلك، تحتاج الوكالة إلى كميات ضخمة من المعلومات المتوافرة لدى الشركات الكبرى لتقديم الخدمات على الإنترنت؛ لأن الشركات تمتلك معلوماتنا وبياناتنا الواضحة غير المشفرة، فهي تتراكم لديها قبل أن يطالها التشفير. ويتطلّب الحصول على معلوماتنا غير المشفرة، أن تخرب الوكالة بروتوكولات الأمن المعلوماتي التي تستعملها مواقع الإنترنت.

هناك دول أخرى منخرطة في ذلك الضجيج المتخالط. ومن المعتقد به على نطاق واسع أن الحكومة الصينية تدسّ مكوّنات لاستراق المعلومات في كل المعدات الشبكية التي تصنعها وتبيعها شركتها «هواوي». وهناك أسباب للاعتقاد بأن المنتجات المشابهة التي تصنعها شركات بريطانية وروسية وإسرائيلية وفرنسية، تتضمن «أبواباً خلفية» لتسريب المعلومات، فرضتها حكومات تلك البلدان⁽⁷⁰⁾.

لا نعرف إذا كانت الحكومات تحاول بخفاء دسّ «أبواب خلفية» لتسريب المعلومات، ضمن منتجات شركات لا تملك حيالها سلطات سياسية أو قانونية، لكن بعض خبراء الكمبيوتر يعتقدون أن الأمور تحدث على ذلك النحو. هل هناك صينيون متحمسون لوطنهم ويعملون في شركات أميركية كبرى لبرامج الكمبيوتر

والإنترنت، وهم يسهّلون للحكومة الصينية سرّاً اختراق منتجات تلك الشركات؟ أم هم المبرمجون الفرنسيون؟ أم هم المبرمجون الإسرائيليون؟ هل على الأقل يسهّلون شيفرة المصدر إلى بلدانهم، ما يسهّل على الأخيرة العثور على نقاط ضعف فيها؟ هل هناك عملاء أميركيون يدسّون «أبواباً خلفية» في الرقاقات الإلكترونية التي تصمّم وتُصنّع في آسيا؟ نعرف أن لديهم موظفين مزروعين سرّاً في بلدان كالصين وألمانيا وكوريا الجنوبية⁽⁷¹⁾؛ كي يساعدوا في زعزعة نظم الكمبيوتر والاتصالات.

استجابت الشركات لتلك الأوضاع باللجوء إلى التطمينات الزائفة المثقلة بالتهديدات القانونية. في سياق مؤتمر تكنولوجيا في العام 2013، حاول إريك شميدت، المدير التنفيذي لـ «غوغل»، تطمين مستمعيه بالقول إنّه «متأكد بدرجة كبيرة من أن المعلومات في «غوغل» آمنة حاضراً، وبمنجاة عن العيون الحكومية المتفحّصة»⁽⁷²⁾. ربما كان أكثر دقة القول: «معلومات بمنجاة عن الحكومة، خلا ما يصيبها بما لا نعرفه من الطُّرق وما لا نستطيع أن نصارحكم بشأنه». ربما بدا ذلك كملاحظة بنبرة لثيمة، لكن طالما كان مسموحاً لـ «وكالة الأمن القومي» أن تستخدم أوامر من المحاكم مستندة إلى تفسيرات سرّية لقانون سرّي، فلن تتبدّل الأوضاع أبداً. بالنسبة للغالبية العظمى من شركات الإنترنت، لا يمثل الأمر مشكلة. ما لم يقله إريك شميدت هو: «وبالطبع، نحن نملك أن ننفذ إلى معلوماتكم وبياناتكم كلها، ونستطيع بيعها لمن نرغب... ولا نجاة لكم من ذلك الأمر». وطالما استمرت الشركات في انخراطها في الرقابة العامة للمستخدمين والمستعملين، يكون من الأسهل عليها أن تتجاوب مع طلبات الحكومة والتشارك في تلك الثروة مع «وكالة الأمن القومي».

وطالما استمرت الحكومات في طلب النفاذ إلى المعلومات، ونأت بنفسها عن وضع تشريعات تحمي تلك المعلومات والبيانات، يكون من الأسهل صنع نظم تسمح بذلك. هناك دورة تغذية قويّة: يدعم نموذج الأعمال جهود الحكومة، وتبرّر جهود الحكومة نموذج الأعمال.

الجزء الثاني

ما هي الرهانات؟

7

العدالة والحرية السياسية

في العام 2013، رفعت «الكنيسة التوحيدية الأولى» في مدينة «لوس أنجلوس» دعوى قضائية ضد «وكالة الأمن القومي»⁽¹⁾؛ بسبب تجسس الأخيرة عليها محلياً، مشيرة إلى رقابة الوكالة على عادات الاتصالات الهاتفية لأعضاء الكنيسة، أدت إلى عزوفهم عن التضامن مع بعضهم بعضاً لدعم قضايا سياسية. لم تكن الكنيسة مصابة بالبارانويا ولا بعقدة اضطهاد. ففي خمسينيات القرن العشرين وستينياته، لاحقت الـ «إف بي آي» رئيس كاتدرائيتها بسبب مواقفه السياسية. وحاضراً، تبدي الكنيسة قلقها من شمول أفراد أميركيين وأجانب في لوائح الرقابة بسبب علاقتهم بتلك الكنيسة⁽²⁾.

تتكلف الرقابة الحكومية غالباً. وبوضوح تام، تظهر الأرقام أنها مكلفة: 72 بليون دولار سنوياً في الولايات المتحدة. وكذلك تكبد مجتمعنا أثراً مرتفعة، محلياً وخارجياً. ويشبه البروفسور يوشاي بنكلر⁽³⁾، وهو أستاذ قانون في «جامعة هارفرد»، رقابة «وكالة الأمن القومي» بأمراض اختلال المناعة الذاتية التي تتسم بأن الجهاز المنوط به صنع مناعة للجسم ضد الأجسام الغريبة عنه، يصيبه خلل وينفلت ليضرب أنسجة الجسم نفسه، ويصبح ذلك الجهاز مصدراً لأمراضه. والأرجح أنه تشبيه جيد.

تشكل الحرية الثمن الأعلى للرقابة، وهو خطر حقيقي ومائل إلى حد أن أناساً من اتجاهات أيديولوجية متباينة باتوا يعربون عن احتجاجهم على توسع الرقابة وتدخلاتها القويّة. وحتى إن مجلة محافظة سياسياً ومؤيدة للأعمال، هي الإيكونومست، ناقشت في مقال افتتاحي في 2013 بأن الرقابة ذهبت بعيداً⁽⁴⁾. وقالت: «وصل الأمر إلى حد أن أحد الاعتقادات الراسخة لدى هذه المجلة؛ وهو ضرورة الترحيب بالتقدم التقني وليس الفرع منه؛ بات في موضع التحدي بمواجهة الحرية. إذ يجب أن تتضمن الحرية بعض الحق في الخصوصية؛ وإذا كان كل ما نفعله موثق في سجلات متسلسلة، تقلص الحرية تماماً».

الإدانة بالمعلومات

في القرن السابع عشر، اشتهر عن السياسي الفرنسي الشهير ريشيليو قوله: «أرني ستة سطور كتبها أشرف رجل في العالم، وأنا كفيل بالعثور فيها على ما يوصله إلى حبل المشنقة». وأعلن لافريتي بيريا، رئيس الشرطة السرية في عهد جوزيف ستالين في الاتحاد السوفياتي السابق: «أرني الرجل، أريك جريمة». قصد ريشيليو وبيريا المعنى عينه: إذا كان لديك معلومات كافية عن شخص ما، بإمكانك العثور على أدلة كافية لإدانته بشيء ما. وللسبب عينه، يحظر القضاء على الشرطة في بلدان عدة، أن ينخرط في «حملات تصيد». وللسبب نفسه وعلى وجه الخصوص، يحظر الكونغرس بصرامة إصدار تفويضات عامة، التي تعني أساساً إعطاء المحققين الحق في البحث عن أي شيء⁽⁵⁾. من المستطاع جعل التفويض العام بالغ الأذى، واستعمله البريطانيون إبان استعمارهم أميركا وسيلة للسيطرة الاجتماعية.

تعني الرقابة الشاملة إمكان إدانة كل شخص بتهمة اختراق القانون، بمجرد أن تعقد الشرطة العزم على ذلك. من الخطورة بمكان العيش في عالم تختزن فيه معلومات عن كل ما تفعله، ثم تقدّم دليلاً ضدك في مرحلة لاحقة من حياتك. هناك خطر واضح في السماح للبوليس بأن يتقّب في تلك التراكمات الهائلة من المعلومات، كي يستخرج

منها «دليلاً» على فعل مخالف للقانون، خصوصاً في بلد كالولايات المتحدة يضم عدّة قوانين عقابية وضبابية، ما يعطي المدّعين سلطة لإدانة من يريدون وبأي تهمة كانت، مع وجود قوانين فضفاضة بشأن ما يمكن أن يكون دليلاً مادياً⁽⁶⁾. ويصح الأمر خصوصاً مع التوسّع في مصطلحات لها وزن قانوني⁽⁷⁾، على غرار جعل «الإرهاب» يشمل الجرائم العادية، و«أسلحة الدمار الشامل» تشمل كل شيء تقريباً بما فيها بنادق الخرطوش. تتسم المصطلحات الأميركية بأنّها فضفاضة إلى حدّ أنّ شخصاً يتبرع بعشرة دولارات للذراع الإنساني في حركة «حماس»، يمكن أن يتهم بالإرهاب⁽⁸⁾.

تجعلنا الرقابة في موضع خطورة بأن يساء إلينا من قبل المسكين بالسلطة، حتى لو لم نكن نفعل أي سوء في الوقت الذي وُضِعنا فيه تحت الرقابة. إنّ تعريف الـ «خطأ» هو شأن اعتباطي، ومن الممكن أن يتغيّر بسرعة. ومثلاً، في حقبة الثلاثينيات من القرن الماضي، كانت الاشتراكية أو الشيوعية اتّجهاً فكرياً رائجاً، أو على الموضة، في الولايات المتحدة، ولم يكن المثقفون يعتبرونها خطأ. تغيّر الوضع بصورة دراماتيكية في خمسينيات القرن العشرين، مع تولي السيناتور جوزيف ماكارثي إطلاق حملات «مطاردة الساحرات»⁽⁹⁾ التي دمّرت الحياة المهنية لكثير من المواطنين الأميركيين المبدئيين والأذكياء، بالكشف عن تاريخهم السياسي. هل سيُنظر إلى الأشخاص الذين يقرأون الآن مواقع «حركة احتلوا وول ستريت»، أو «حزب الشاي»، أو حقوق الحيوان أو الحق في حمل السلاح، بوصفهم متّهمين بممارسة نشاطات إرهابية بعد خمس أو عشر سنوات؟

ويزيد في سوء ذلك الوضع أننا نُولد كمّيّات كبيرة من البيانات التي تختزن إلى الأبد. وتستطيع «حملات التصيّد» أن تعود إلى الماضي، وتعرّ على أشياء فعلتها قبل 5 أو 10 أو 15 أو 20 سنة، وما زال العدّد مستمراً. يستطيع جيل الكبار حاضراً أن ينجو من تهوّارته في مرحلة المراهقة. لن يمتلك المراهقون حاضراً تلك الميزة؛ لأن حياتهم كلها ستكون موثّقة في سجل أبدي.

(*) إشارة إلى حملات أطلقها متشدّدو الكنيسة الكاثوليكية في أوروبا في القرون الوسطى، وأعدمت فيها نساء كثيرات بدعوى كونهن ساحرات متّصلات بالشیطان.

ثمة ضرر آخر ينجم من الرقابة الحكومية يتمثل في طريقة تصنيف الناس لممارسة التمييز ضدهم. ويصف البروفسور دانيال سولوف، وهو أستاذ قانون من «جامعة جورج واشنطن»، ذلك الوضع بأنه «كافكاوي»⁽⁹⁾. «ففي سرية، يُجمع معظم تلك البيانات ويستخدم، ولا نملك الحق في دحض تلك الأدلة المستخدمة ضدنا، بل ولا حتى رؤيتها. ولسوف يزداد الأمر سوءاً عندما تبدأ النظم المؤتمتة في تحليل بيانات الرقابة واتخاذ القرارات المستندة إليها، بصورة أوتوماتيكية تماماً.

استُخدِمت بيانات الرقابة ومعلوماتها في تبرير عدد من العقوبات، بداية من تعريض الناس إلى إجراءات أمنية مشددة ووصولاً إلى ترحيلهم⁽¹⁰⁾. في 2012، قبل انطلاقه لقضاء عطلة في «لوس أنجلوس»، غرّد الشاب الإيرلندي لي فان برايان⁽¹¹⁾ على «تويتر» قائلاً: «أنا حرّ هذا الأسبوع، كي أنجز بعض النسيمة/ التحضير، قبل أن أذهب لتدمير أميركا». كانت الحكومة الأميركية ترصد تغريدات «تويتر» كافة⁽¹²⁾. التقط عملاء حكوميون تلك التغريدة، وقارنوها مع لوائح القادمين إلى أميركا جواً، وكانوا بانتظار ذلك الشاب في المطار عند وصوله من إيرلندا. لم تكن كلماته سوى مزاح، لكنه خضع لاستجواب دام 5 ساعات قبل إعادته إلى بلاده⁽¹³⁾. نعرف أن التنكيت في المطارات عن التفجيرات تعرّض صاحبها للاعتقال. وحاضراً، يبدو أنه صار واجباً الحذر عند إصدار وعود ضبابية عن مشاكسة دولية، في أي مكان على الإنترنت⁽¹⁴⁾.

في 2013، وضع شخص من جزيرة «هايتي» يظهر فيه وهو يتناول مشروباً روحياً أثناء قيادة سيارته. اعتقلته الشرطة بسبب تلك الجريمة⁽¹⁵⁾. ودافع الرجل عن نفسه بالإشارة إلى أن الأمر كان تمثيلاً، والشراب الذي كان يتناوله لم يكن كحولياً.

(*) إشارة إلى روايات الكاتب الشهير فرانز كافكا التي تتميز بأجوائها الكابوسية والمأساوية والعبيثية، مع إحساس شامل بالضيق الوجودي.

حدثت أمور أشد سوءاً في المملكة المتحدة. إذ سُجِنَ بعض الناس هناك بسبب تغريدة عنصرية⁽¹⁶⁾، أو تدوينة هاذرة على «فيسبوك»⁽¹⁷⁾. وبالطبع، الأرجح أن الأمر أكثر سوءاً بما لا يقاس في بلدان أخرى اعتادت على سجن الناس وتعذيبهم بسبب أشياء كتبوها على الإنترنت.

يصل القلق إلى أقصاه عند تذكّر أن الجيش الأميركي يوجّه غارات الـ «درون» استناداً إلى معلوماته عمن يستهدفهم القصف⁽¹⁸⁾. هناك نوعان من التوجيه للـ «درون»: يسمّى الأول «القتل الموجه»، يحدّد فيه الشخص المستهدف بواسطة الرقابة الإلكترونية أو سواها. يطلق على الثاني تسمية «القتل بالتوقيع»⁽¹⁹⁾؛ نظراً لاستهدافه أشخاصاً مجهولين يجري تحديدهم وفقاً لسلوكهم وسماتهم الشخصية، كعمرهم ونوعهم الجنسي ظاهرياً، وموقعهم جغرافياً، وما يبدو أنهم منخرطون في فعله. عندما وصلت غارات الـ «درون» إلى زرونها في باكستان عامي 2009 و2010، شكّل «القتل بالتوقيع» نصف غارات الـ «درون»⁽²⁰⁾. لا نملك معلومات عن مدى دقة رسوم الملامح الشخصية («بروفایل») التي استندت تلك الغارات إليها.

إنّه خطأ كامل. يجب أن نكون أحراراً عند الحديث مع أصدقائنا، أو بثّ رسالة نصيّة إلى أحد أفراد العائلة، أو قراءة كتاب أو مقال، من دون مكابدة القلق من رأي الحكومة المحتمل في تلك الأمور: سواء الحكومة حاضراً، أو بعد 5 أو 10 سنوات، أو حتى حكومات أخرى. يجب ألا نقلق حيال احتمال فهم أو إساءة فهم أفعالنا، أو أنها ربما تستعمل ضدنا. يجب ألا نكون عرضة لرقابة من دون حدود⁽²¹⁾.

الحجب الحكومي

تعتمد الحرية أيضاً على حرية تداول الأفكار. ويخنق الحجب الحكومي المتآزر غالباً مع الرقابة الإلكترونية والحرية والأفكار معاً.

تحمي الصين مواطنيها من «مخاطر» الأخبار الأجنبية والأفكار الآتية بواسطة الإنترنت، بما ما يسمّى «الدرع الذهبي» (Golden Shield)، بالأحرى «جدار النار الصيني العظيم» (Great China Firewall) ⁽²²⁾، في إشارة إلى «جدران النار» الإلكترونية التي هي برامج لرقابة الحركة على الإنترنت.

واستغرق إنجاز ذلك المشروع الضخم 8 سنوات، بتكلفة بلغت 700 مليون دولار. وتتمثل مهمته في فرض الحجب على الإنترنت. ويشكل منع الأفكار المضرة وخنق حرية الكلام أهدافاً ثانوية له ⁽²³⁾، فيما يتمثل هدفه الرئيس في منع نشوء منظمات فعالة. يعمل ذلك «الجدار الناري» بصورة جيدة ⁽²⁴⁾؛ لأن من لديهم تمرساً في التقنيات الإلكترونية يستطيعون تفاديه، لكنه يمنع غالبية الشعب الصيني من العثور على أشياء كثيرة، بداية من المعلومات عن دالاي لاما، (القائد الروحي لشعب التيب)، ووصولاً إلى مجموعة من مواقع محرّكات البحث الغربية.

ثمة حجب حكومي يمارس على الإنترنت حاضراً أكثر من أي وقت مضى ⁽²⁵⁾. ولا يتعلّق الأمر بالسياسة وحدها. هناك بلدان تحجب مواقع إلكترونية بسبب طبيعتها الجنسية، أو الأفكار الدينية التي تنشرها، أو استضافتها لمنصات لعب القمار، أو ترويجها لمواد مكيفة أو نشاطات غير شرعية. تعيش غالبية مواطني الشرق الأوسط تحت حجب حكومي واسع. تحجب فرنسا وألمانيا والنمسا أفكار النازيين الجدد ⁽²⁶⁾، بما فيها المزايدات على مقتنيات تعود إلى الحقبة النازية، فيما تفرض بلدان أخرى حجباً على المواقع التي تعرّض على العنف. ويمنع «التشريع 72» الفيتناميين من نقاش أمور عامة على الإنترنت ⁽²⁷⁾. وتحجب بلدان كثيرة المحتوى المخالف لقوانين الملكية الفكرية ⁽²⁸⁾. ويعدّ حجب المواقع الإباحية جنسياً أمراً بديهياً في بريطانيا، على الرغم من وجود خيار بالخروج من ذلك الحجب ⁽²⁹⁾. وفي 2010، حجبت الولايات المتحدة موقع «ويكيليكس» ⁽³⁰⁾.

يحظى معظم الحجب بدعم من الرقابة، ما يؤدي إلى فرض حجب ذاتي. إذا علم الناس أن الحكومة تراقب كل ما يقولونه، يصبحون أقل ميلاً لقراءة مواضيع محظورة أو حتى الحديث عنها. شكّل ذلك هدفاً لقانون أصدرته روسيا في 2014، يطلب من أصحاب المدونات الإلكترونية «بلوغرز» (Bloggers) التسجيل لدى الحكومة⁽³¹⁾. ويفسّر ذلك أيضاً سبب نجاح «جدار النار الصيني العظيم» كأداة للحجب؛ إذ لا يعود ذلك إلى القدرات التقنية لذلك الجدار وحدها، بل أيضاً إلى الخطر الذي يتهدّد من يحاول تفاديه، بأن مواطنين آخرين للحكومة ربما اكتشفوه وأبلغوا عنه. لا يعني ذلك أن أولئك المُبلّغين هم بالضرورة متوافقون مع الحكومة⁽³²⁾، بل إنهم يخشون أن يعاقبوا إن هم لم يبلغوها عن المخالفين. وفي الصين، تفرض شركات الإنترنت حجبا على مستخدميها يفوق المطلوب منها رسمياً⁽³³⁾.

وكلما زادت العقوبات على من يُضبط متهرباً من رقابة الحكومة، زاد الميل إلى ممارسة الحجب الذاتي⁽³⁴⁾.

تأثيرات مفزعة

تملك الرقابة تأثيرات مفزعة في المجتمع⁽³⁵⁾. لاحظت ذلك سونيا سوتومايور، القاضية في «المحكمة الأميركية العليا»، أثناء إبدائها رأيها في قضية رفعت في العام 2012، بشأن دسّ الـ «إف بي آي» جهازاً للتتبع متّصل بالـ «جي بي إس» في سيارة أحد الأفراد. إذ قالت سوتومايور: «يؤدي التنبّه إلى احتمال وجود رقابة حكومية، إلى إثارة فزع بشأن حريّتي التعبير والترابط. لكن القدرة غير المحدودة للحكومة في جمع معلومات تكشف مناحي خصوصية عند الأفراد، هي عرضة لإساءة الاستخدام. وتكون المحصلة النهائية أن التتبع بالـ «جي بي إس» يوفر بتكلفة بسيطة كميات أساسية من المعلومات عن كل شخص ترغب الحكومة في تتبعه⁽³⁶⁾، مع غياب الضوابط المناسبة؛ ولربما أثر ذلك في علاقة المواطن مع الحكومة بطريقة لا تتلاءم مع المجتمع الديمقراطي».

كتب البروفسور إيبين موغلن، وهو أستاذ قانون في «جامعة كولومبيا»، عن مسألة الرقابة، لافتاً إلى «أنّ الحضور الشامل للتنصّت المتعدي، هو أمر يخلق الخوف الذي هو العدو للحرية المنظمة العاقلة»⁽³⁷⁾.

في الولايات المتحدة، بدأنا في رؤية بواكير ذلك الفزع. ووفق تقرير لمنظمة «هيومن رايتس ووتش»، أعاقَت الرقابة الحكومية كتابة الصحفيين عن مجتمع الاستخبارات، الأمن القومي، وقوى إنفاذ القانون، إذ باتت المصادر أقل ميلاً للاتصال بهم، بل صاروا هم أنفسهم يخشون الملاحقة والإدانة⁽³⁸⁾. واستنتجت «هيومن رايتس ووتش» أن هناك قصصاً تقضي المصلحة الوطنية بالكتابة عنها، لكن لم يجز تناولها إعلامياً، ما يعني أن الجمهور أصبح على درجة أقل من الدراية والمعرفة. ذلك هو بالضبط الأثر المفزع الذي تولّده الرقابة.

وتأثر بالأمر عينه المحامون الذين يعملون على قضايا لها صلة ما بالاستخبارات⁽³⁹⁾، كالإرهاب والمخدرات ووكلاء الحكومات الأجنبية. وعلى غرار الصحفيين، بات المحامون يخشون أن تراقب محادثاتهم، وأن تصل حواراتهم مع موكلهم إلى أيدي الادعاء⁽⁴⁰⁾.

عقب 9 / 11، أوصلت الرقابة الكتاب إلى فرض حجب ذاتي على أنفسهم⁽⁴¹⁾. إذ تجنّبوا الكتابة عن موضوعات معينة وإجراء تحقيقات بشأنها، وصاروا حذرين عند الاتصال مع المصادر والزملاء، بل حتى أصدقائهم في الخارج. وأظهر استطلاع أجراه «مركز بيو للبحوث» عقب نشر الوثائق الأولى لسنودن، أنّ الناس لم يعودوا راغبين بالحديث عن «وكالة الأمن القومي» على الإنترنت⁽⁴²⁾. وكذلك بين استطلاع أكثر توسّعاً أجراه «مركز هاريس» أن نصف الأميركيين غيروا موضوعات البحث والقراءة والمحادثة بواسطة الإنترنت؛ بسبب رقابة «وكالة الأمن القومي»⁽⁴³⁾. أدت الرقابة إلى فزع من استخدام الإنترنت لدى المسلمين الأميركيين⁽⁴⁴⁾، ومجموعات البيئة⁽⁴⁵⁾، ومناصري الحق في حمل السلاح، ومن ينشطون بشأن سياسات مكافحة

المخدرات، والعاملين في مجال حقوق الإنسان. وعقب كشافات سنودن في 2013، صار الأفراد في أنحاء العالم أقل ميلاً لوضع تعابير شخصية حساسة على محرك البحث «غوغل»⁽⁴⁶⁾.

في 2014، لاحظ تقرير «المفوضية العليا لحقوق الإنسان في الأمم المتحدة» أن «مجرد التلويح باحتمال أن تلتقط بيانات الاتصالات، يؤدي إلى الإخلال بالخصوصية، مع إمكان حدوث تأثيرات مفرغة في الحقوق، وضمنها الحق في التعبير وتكوين الروابط»⁽⁴⁷⁾.

لا يتعلق الأمر بعقدة اضطهاد مرضية وهذيان البارانونيا. في إحدى حملاته الانتخابية في 2012، أشار الرئيس الفرنسي نيكولا ساركوزي إلى أن «كل شخص يتردد بانتظام على مواقع شبكية منحازة للإرهاب أو تنشر الكراهية، سوف يحكم عليه بالسجن»⁽⁴⁸⁾.

لا يقتصر الخوف من التمهيص على أفعال الحاضر وحدها، بل تشمل الماضي أيضاً. إذ بات السياسيون يعيشون في عالم تلاحقهم فيه كاميرات المعارضة باستمرار، على أمل تسجيل ما يمكن وضعه خارج السياق. وتحاكم في الحاضر كل الأشياء التي قالوها في الماضي، وبدقة أكبر مما كان متخيلاً قبل سنوات قليلة. تخيل لو أن الأمر عينه ينطبق على كل من يسعى إلى وظيفة ما.

بالطبع، لا يتأثر الناس بالرقابة بشكل متساو. لا يعير بعضنا بالاً للرقابة الحكومية، ولا يتأثر بها كلياً. في المقابل، يتأثر بعضنا كثيراً، خصوصاً من ينتمون إلى مجموعات دينية، واجتماعية، وإثنية واقتصادية لا تروق للنخبة الحاكمة.

تتمحور الملاحظة الرئيسة للكاتب جيرمي بنثام بخصوص الـ «اوبتيكون» (راجع الفصل 7)، حول فكرة أن الناس يصبحون مطواعين وموالين عندما يعتقدون بأنهم مراقبون. يشكل الـ «اوبتيكون» هندسة للسيطرة الاجتماعية. فكّر في طريقة تصرفك عندما تسير سيارة بوليس بمحاذاة سيارتك، أو في حال بلد برمته حين

يتولّى موظفو الحكومة التنصّت على مكالماتهم⁽⁴⁹⁾. عندما نعرف أن كل شيء يجري تسجيله، نغدو أقل ميلاً للحديث بصراحة والتصرف إفرادياً. عندما نكون تحت تهديد دائم بالمحاكمة والنقد والعقاب على تصرّفاتنا، يتتابنا خوف من أنه، إما الآن أو في مستقبل غير محدّد، سوف تستحضر البيانات التي خلّفناها وراءنا، كي تديننا بواسطة أي شيء تركّز عليه الحكومة يومئذٍ من التصرفات التي عدناها ذات مرّة بريئة وخصوصيّة. وكردّة فعل، لا نفعل شيئاً خارج المألوف. نفقد خصوصيّتنا، فيما تركّز حركة المجتمع. لا نساثل السلطة ولا نتحداها. نغدو مطيعين ومستسلمين. نصبح أقل حرّة.

منع التمرد والتغيّر الاجتماعي

تملك تلك التأثيرات المثيرة للفرع وقعاً مدمراً في الخطاب السياسي بوجه خاص. هناك قيمة للتمرد⁽⁵⁰⁾. وربما امتلك خرق القانون بعض القيمة أيضاً، مهما بدا القول غريباً. ويعمل التمرد وخرق القانون على تحسين المجتمع. إنّ الرقابة الشاملة الكلية القدرة هي العدو للديمقراطيّة، والحرية، والتقدّم والتحرّر.

يتطلّب الدفاع عن ذلك التأكيد دفاعاً قوياً ومرهفاً - هو ما فعلته في كتابي السابق كذّبة وتمرّدون⁽⁵¹⁾ - لكنه يمتلك أهمية حيويّة للمجتمع. لنفكر بالأمر على النحو التالي: بالولايات المتحدة، ثمة ولايات صارت على شفا تغيير قوانين راسخة منذ عقود بصدد العلاقات المثليّة جنسياً وكذلك استخدام الماريجوانا (حشيشة الكيف). لو أن الرقابة عضّدت القوانين القديمة لما تغيّرت، وما كنا لنصل إلى حدّ أن معظم المواطنين باتوا يقبلون تلك الأمور. لا بد أن توجد مرحلة تكون فيها الأمور غير شرعيّة لكن يجري تقبّلها باطراد، ما يدفع الناس إلى التلقّف حولهم قائلين: «أتعرف؟ إنّها ليست سيّئة تماماً». صحيح أن تلك العملية تستغرق عقوداً، لكنها لا توجد أصلاً من دون اختراق القوانين. وصرّح الموسيقار والمفكر الأميركي فرانك

زابا بشيء مماثل في 1971، قائلاً: «دون الخروج عن العرف السائد، يضحى التقدم مستحيلاً»⁽⁵²⁾.

يؤدي الإنفاذ الكامل للقوانين بمساعدة الرقابة إلى شلل في تلك العملية. نحن بحاجة إلى أمن منقوص⁽⁵³⁾، بمعنى وجود نُظُم تترك الحرية للناس كي يجربوا أشياء جديدة، بطريقة تشبه ما تحدثه جلسات العصف الفكري غير الموثقة، من تليين للكوابح وتدعيم للابتكار. دون ذلك، يصبح مستحيلاً التدرج من وضع تكون فيه أشياء غير شرعية ومرفوضة، إلى وضع تغدو فيه شرعية لكن مع شيء عدم التيقن بشأن رفضها، إلى الاستمرار في كونها غير شرعية لكنها مقبولة على الأرجح، ثم الانتهاء إلى جعلها شرعية.

من المهم ملاحظة ذلك الأمر. هناك حريّات ننعم بها حاضراً لكنها كانت في زمن ماضٍ تعتبر مهدّدة أو حتى جرميّة، بعيون السلطة الحاكمة آنذاك. ما كانت تلك التغيّرات لتحدث أبداً لو أن السلطات امتلكت القدرة على تحقيق السيطرة الاجتماعية بالرقابة.

يشكّل ذلك أحد الأسباب الرئيسة كي نهتم جميعاً بشأن التركيبة الصاعدة حاضراً للرقابة، حتى لو لم تصبنا آثارها المفزعة بصور شخصية. إذ نعاني تلك الآثار لأن الناس حولنا يصبحون أقل قدرة على تبني أفكار سياسية أو اجتماعية جديدة، أو التصرف بطرق غير مألوفة. لو نجحت رقابة السيناتور المتشدد جوزيف مكارثي في إخماس صوت داعية الحقوق المدنية الأفريقي - الأميركي القس مارتن لوثر كينغ، لترك الأمر آثاراً تطال ما هو أبعد من كينغ وأسرته.

بديهي القول إن ثمة أشياء غير شرعية ستبقى غير شرعية للأبد: كالقتل والسرقعة وما إلى ذلك. في المقابل، يولد التطرف في دقة إنفاذ القانون، تداعيات غير مسبوقة. ماذا يعني للمجتمع أن تكون الشرطة قادرة على متابعة سيارتك على مدار الساعة، وإرسال فواتير لك في آخر الشهر تتضمن كل مرة زدت فيها من سرعتك، أو

تجاوزت إشارة حمراء، أو انعطفت إلى اليسار بالخطأ، أو لحقت بالسيارة التي أمامك من مسافة قريبة جداً؟ ماذا يعني أن تكون السلطة المحلية في بلدتك قادرة على استعمال الصور الجوية بطريقة أوتوماتيكية⁽⁵⁴⁾، لتوقع عليك غرامة كلما تأخرت في جزّ عشب حديقتك، أو ربما لم تنتظم في مشيتك؟ يستند نظامنا القانوني على محاكمة الأمور إنسانياً. وفيما تحيق المخاطر بالأحكام المسبقة والمنحازة، فهناك مخاطر أكبر من إبدال تلك الأحكام بمحض جداول خوارزمية تعمل بكفاءة⁽⁵⁵⁾.

ثمة احتمال بأن تقود الرقابة الشاملة إلى مجتمع من النوع الذي رسمه فيلم «تقرير الأقلية» (ظهر في 2002، من بطولة الممثل توم كروز)، بمعنى أن يضحي الناس عرضة للخضوع إلى تحقيق بوليسي قبل إتيانهم بأي جرم⁽⁵⁶⁾. وفعلياً، بدأت وكالات إنفاذ القانون في استخدام أدوات تحليلية استباقية للتعرف إلى المشتبه فيهم، وكذلك لتوجيه التحقيقات⁽⁵⁷⁾. ولم تعد سوى خطوات قصيرة تفصلها عن الوصول إلى مجتمع «الأخ الكبير» وجرائم الفكر.

إنّ مفهوم جعل الإفلات من جرائم معينة أمراً مستحيلاً، هو جديد⁽⁵⁸⁾ - مع احتمال كونه ناجماً عن تلك التقنيات المتقدمة كلها - ويجدر التفكير فيه بحذر وتروّ قبل وضعه موضع التنفيذ. ووفق تعبير البروفسور يوشاي بنكلر: «النقص عن الكمال هو بُعدٌ أساسي في الحرية»⁽⁵⁹⁾.

زحف السرية

تتمرد السرية عموماً على الرقابة الحكومية، وكذلك تمثل خطراً على المجتمع الحر والمفتوح.

في الولايات المتحدة، عبّر ذلك عن نفسه بصور متنوعة، إذ وسّعت الحكومة تعريف ما يمكن اعتباره سرّاً. تتمثل إحدى حقائق الأمن القومي في كون السرية ضرورية في شؤون الاستخبارات والدفاع والسياسة الخارجية⁽⁶⁰⁾. إذا كشفت

الحكومة أشياء معينة- كتحرّكات الفرق العسكرية، وقدرات الأسلحة والمواقف الفعلية في المفاوضات- يتمكن العدو من تغيير تحرّكاته بما يخدم مصلحته. استمرت صحة ذلك المفهوم للسرية العسكرية طيلة آلاف السنوات⁽⁶¹⁾، لكنه تغيّر حاضراً بشكل دراماتيكي⁽⁶²⁾. أنا أستعمل الولايات المتحدة كنموذج عن ذلك. في الحرب العالمية الأولى، كنّا منشغلين بسرية وقائع محدّدة، كمواقع الوحدات العسكرية والخطط التفصيلية للمعارك. في الحرب العالمية الثانية، جرى توسيع مفهوم السرية ليشمل عمليات واسعة النطاق ومساحات كاملة من المعرفة، كليهما معاً⁽⁶³⁾. إذ لم يقتصر الأمر على سرية برنامجنا لبناء قنبلة ذرية، بل إن كامل الحقول العلمية المتعلقة بالسلح النووي عُدت سرية أيضاً⁽⁶⁴⁾. عقب 9 / 11، عمّمنا المفهوم كثيراً⁽⁶⁵⁾. وحاضراً من المستطاع وصف أي شيء تقريباً بأنه سرّ.

وبالنتيجة، تفجّرت سرية الحكومة الأميركية. لا أحد يعرف الرقم الدقيق⁽⁶⁶⁾ - لأنه سرّ بالطبع - لكن التقديرات تشير إلى أن بلايين الصفحات من الوثائق الحكومية الأميركية، توضع في خانة السرية سنوياً. في الوقت عينه، تكاثرت كالفطر أعداد الأشخاص الممنوحين أذونات أمنية. وفي تشرين أول / أكتوبر 2012، حاز قرابة 5 ملايين شخص في الولايات المتحدة أذونات أمنية⁽⁶⁷⁾ (من بينهم 1.4 مليون مصنفون في خانة «سري جداً»)، ويساوي ذلك زيادة بـ 50٪ عما كانه في 1999.

توضع في خانة السرية تفاصيل الرقابة كافة التي تمارسها «وكالة الأمن القومي» خشية أن تتسرّب إلى الأشرار⁽⁶⁸⁾. (سأعود إلى تلك المحاجة في الفصل 13). قبل كشوفات سنودن، لم يكن متاحاً قراءة التوجيهات السياسية الرئاسية التي خوّلّت لـ «وكالة الأمن القومي» معظم أعمالها في الرقابة. لم يكن مسموحاً حتى بقراءة أوامر المحكمة التي تتخصّص بتحويل أعمال تلك الرقابة⁽⁶⁹⁾. كانت تلك الأمور سرية كلها، وكانت لتبقى كذلك لولا أن كشوفات سنودن أدّت إلى رفع غطاء السرية الحكومية عن حفنة منها.

لا تقتصر زيادة مستويات السرية على الجيش و«وكالة الأمن القومي» وحدهما. إذ شرعت قوى إنفاذ القوى القانون محلياً في تلبية مراقبتها الخاصة برداء السرية. ومثلاً، صار طلب الشرطة رقابة هاتف خلوي ما أمراً روتينياً، تصادق عليها المحاكم التي تخوله تلك السلطة⁽⁷⁰⁾. (لا تعترف الشرطة في المملكة المتحدة ولو بمجرد أنها تستخدم تلك التقنية)⁽⁷¹⁾. وهناك أمثلة كثيرة عن ذلك.

توهن تلك السرية الضوابط والكوابح الموضوعية للإشراف على الرقابة، وكذلك، بصورة أوسع، التثبت من كوننا نعامل جميعاً بعدالة من قبل قوانيننا. منذ هجمات الإرهاب في 9/11، صارت الرسائل الأمنية للـ «إف بي آي» و«وكالة الأمن القومي»، تأتي مرفقة بحظر قضائي. إذ يُمنع من يتلقى تلك الرسائل من الحديث عنها، حتى بتعابير عمومية⁽⁷²⁾. ويصعب ذلك أمر مقارعة تلك الرسائل في المحاكم.

تختبئ الحكومات أيضاً خلف اتفاقيات مع الشركات بعدم التصريح. وتستند الـ «إف بي آي» وقوات الشرطة المحلية على تلك الاتفاقيات في عدم الإفصاح عن طريقة عمل نظام «ستنغراي» (راجع الفصل الخامس) في رقابة الهواتف الخلوية⁽⁷³⁾. وتلجأ قوات الشرطة المحلية إلى الممارسة عينها في رفضها كشف تفاصيل الجداول الخوارزمية المستخدمة في أدوات التحليل الاستباقية، التي تستخدم في تدخلات ضباط الشرطة⁽⁷⁴⁾.

عبّرت سرية الحكومة عن نفسها بطريقة ثانية، وهي كونها دُفِعت إلى درجة قصوى. تملك الولايات المتحدة إطاراً قانونياً معقداً في التصنيف، لكن يجري تجاهله باطّراد⁽⁷⁵⁾. وتسيء السلطة التنفيذية استعمال الصلاحيات التي تحوزها لإبقاء المعلومات العامة بعيدة عن أعين العموم⁽⁷⁶⁾. تنأى السلطة التنفيذية بأسرارها عن الكونغرس⁽⁷⁷⁾. وتحفظ «وكالة الأمن القومي» بأسرارها بعيدة عن يناط بهم مهمة الإشراف على الوكالة⁽⁷⁸⁾، بما في ذلك الكونغرس⁽⁷⁹⁾. يكتّم بعض

أعضاء الكونغرس أسراراً عن بقية أعضاء الكونغرس⁽⁸⁰⁾. وتحفظ المحاكم السرية بأسرارها لنفسها⁽⁸¹⁾، وحتى «المحكمة العليا» صارت أكثر ميلاً لإبقاء وثائقها طي السرية⁽⁸²⁾. في واشنطن، تعدّ المعرفة نقوداً، ويعتمد مجتمع الاستخبارات إلى مراكمتها.

تأتي العلامة الثالثة على سرية الحكومة من واقع أنها تعاملت بقسوة تامة مع أولئك الذين كشفوا أسرارها: لنسميهم «مُطلقو صافرات الإنذار». أبدى الرئيس باراك أوباما حماسة خاصة في محاكمة الأفراد الذين كشفوا الأعمال الخاطئة للوكالات الحكومية⁽⁸³⁾. ومنذ انتخابه في العام 2008، أصر على محاكمة ثمانية أشخاص بسبب كشفهم معلومات سرية إلى الصحافة. كان الرقم عينه هو ثلاثة أشخاص منذ إقرار «قانون التجسس» في العام 1917⁽⁸⁴⁾.

في القانون الأمريكي، لا يعدّ إطلاق صافرة إنذار لتنبية الجمهور عذراً مقبولاً في ما يتعلق بالاستخبارات؛ إذ يمنع «قانون التجسس» الشخص المدعى عليه من شرح سبب تسريبه معلومات سرية. كان دانيال إل سبرغ هو أول من حوكم تحت ذلك القانون في العام 1971، ومُنِع من تفسير أعماله أمام المحكمة. وعندما حوكم توماس درايك، وهو مدير تنفيذي سابق في «وكالة الأمن القومي»، مُنِع من استخدام تعبري «إطلاق صافرة إنذار» و«الإفراط في السرية» أثناء محاكمته⁽⁸⁵⁾. وكذلك مُنِعَت تشيلسا مانغ(*) من استخدام دفاع مماثل أثناء محاكمتها⁽⁸⁶⁾.

ادّعى إدوارد سنودن أنّه من مُطلق صافرات الإنذار⁽⁸⁷⁾. ويوافق كثيرون، وأنا منهم، على ذلك الزعم، فيما يرفضه آخرون. وأصرّ وزير الخارجية جون كيري على وجوب «أن يعود سنودن إلى بلاده، ويقف أمام نظامنا القضائي، ويدافع عن قضيته»⁽⁸⁸⁾. وكذلك زعمت وزيرة الخارجية السابقة هيلاري كلينتون أنّه «إذا أراد

(*) حوكت في قضية «ويكيليكس» لأنها سربت وثائق سرية عندما «كانت» جندياً يعمل في المعلوماتية اسمه برادلي مانغ الذي طلب تغيير جنسه في خضم محاكمته، وتحول إلى الأنثى تشيلسا.

سنودن أن يعود مع علمه أنه يتحمل مسؤولية أفعاله ويستطيع الدفاع عن نفسه، سيجب عليه اتخاذ ذلك القرار بنفسه»⁽⁸⁹⁾. يقدم التصريحان كلاهما نموذجاً عن نفث دخان التضليل السياسي⁽⁹⁰⁾. إذ لا يتيح القانون الساري حاضراً لسنودن أن يدافع عن نفسه.

وبقدر ما تتطلبه الرقابة الحكومية من سرية، يفقد الناس سلطة النقاش والتصويت على ما تفعله حكومتهم باسمهم، أو الإفصاح إلى من يتخبونهم عما يفكرون أنه يجب القيام به. من السهل نسيان، في خضم السيل الطامي من العناوين الإعلامية عن «وكالة الأمن القومي» وبرامجها في الرقابة، أن أحداً ما كان يعلم شيئاً عنها، لولا أن سنودن كشف ما كانت تفعله الوكالة، متحملاً أكلافاً ومجازفات شخصية كبرى.

إساءة استعمال

في وقت مبكر من العام 2014، استهل شخص ما حساباً تهكمياً على «تويتر»، مستخدماً اسم جيم آرديس، عمدة بلدة «بيوريا» بولاية «إلينوي». كان تهكماً مؤذياً إلى حد كبير، ما أثار حفيظة آرديس. وأدى غضبه إلى إطلاق سلسلة من الحوادث، تضمنت حصول الشرطة المحلية بطريقة غير مشروعة على أمر قضائي يفرض على «تويتر» تسليم معلوماته عن شخصية ذلك الشخص⁽⁹¹⁾، ثم أغارت الشرطة على بيته، واعتقل جون دانيال. لم تُسَقِّ تهم ضد دانيال، أساساً لأن الأخير لم يقم بأعمال غير قانونية. وحاضراً، يتابع «الاتحاد الأميركي للحريات المدنية» دعوى قضائية ضد بلدة «بيوريا» لمصلحة دانيال.

إنّ نظم الرقابة كلها عرضة لإساءة الاستعمال. في السنوات الأخيرة، استعملت الشرطة الرقابة لاستفزاز المعارضة، وكذلك للتحرش بأناس ترغب في مضايقتهم، كما كان الحال مع دانيال. هناك مثل عن ذلك حدث في 2014؛ إذ اعتادت الشرطة في «نيو جيرسي» روتينياً أن تلتقط صوراً للمحتجين في المناسبات التي يستضيفها

حاكم الولاية كريس كريستي، إلى أن أصدر مدّعي عام الولاية أمراً قانونياً يوقف تلك الممارسة⁽⁹²⁾. وفي العام 2014 أيضاً، بتنا نعرف أن الـ «سي آي إيه» اخترقت أجهزة كومبيوتر يملكها موظفون في «لجنة الاستخبارات في مجلس الشيوخ» التي كانت تدقّق في أعمال الـ «سي آي إيه». وصرنا نعرف أنّه في 2013، تجمّست «وكالة الأمن القومي» على اتّصالات الأمم المتحدة، مخترقة بذلك القانون الدولي⁽⁹³⁾. نعرف أن إساءة استعمال من الأنواع كافة حدثت من قِبَل سلطات الرقابة المحلية في الولايات، وعلى المستوى القومي أيضاً.

تحدث أصناف من إساءة الاستعمال داخل منظمات الرقابة نفسها أيضاً. ومثلاً، درج موظفو «وكالة الأمن القومي» على التنصّت على المكالمات الهاتفية الشخصية للأميركيين في دول أجنبية، واعتراض رسائل الـ «إيميل»، كما تداولوا الصور ذات الإيحاءات الجنسية الفوّارة بين مكاتبهم. جاءت تلك المعلومات من شخصين كانا يعملان في اعتراض البريد الإلكتروني في 2008⁽⁹⁴⁾، ومرة أخرى من سنودن في 2014⁽⁹⁵⁾. ونعرف من وثائق «وكالة الأمن القومي» أنّ عملاءها تجسّسوا أحياناً على أشخاص يعرفونهم في الولايات المتحدة، وكانوا يسمّون تلك الممارسة «لوف إنت» (LOVEINT)⁽⁹⁶⁾. وتلاحظ وثائق التدقيق في أعمال الوكالة أنها اخترقت بنفسها قواعد عملها في 2276 مرّة خلال 12 شهراً، بين عامي 2011 و2012⁽⁹⁷⁾. إنّه رقم مرتفع - ثمانية اختراقات يومياً - لكن الرقم الحقيقي ربما كان أكبر بكثير⁽⁹⁸⁾. وبأثر من الطريقة التي تراقب فيها الوكالة عملها، تستطيع الوكالة أن تحدّد عدد الاختراقات التي تستطيع اكتشافها.

ليست تلك بمشكلة جديدة، ولا تقتصر على «وكالة الأمن القومي». إذ يُظهر التاريخ الأمريكي الحديث وجود مراحل من الإساءة الممنهجة لاستعمال الرقابة: ضد قادة العمال ومن المشتبه فيهم بأنهم شيوعيون، في مرحلة ما بعد الحرب العالمية

الأولى؛ وضد قادة حركة الحقوق المدنية^(*) والمحتجّين على الحرب في فيتنام. ليست التفاصيل المحدّدة عن تلك المراحل بجذابة، لكن يمكن الحديث عن اثنين منها.

• بفضل الرقابة المكثّفة، عرف السيناتور ج. إدغار مكارثي بوجود علاقات عاطفيّة للقس الأفريقي - الأميركي مارتن لوثر كينغ خارج رباط الزوجيّة، وخطّ رسالة مُغفلة المُرسَل محاولاً دفعه إلى الانتحار في العام 1964⁽⁹⁹⁾، إذ ورد فيها: «كينغ. انظر إلى قلبك. تعلم أنك فاسد كلياً وتمثّل إساءة لنا نحن الزوج جميعاً. يحصل البيض في هذه البلاد على ما يكفيهم من الفساد، لكنني واثق بأنهم لا يملكون شخصاً يمثل فسادك. أنت لست رجل دين، وتعرف ذلك جيّداً. أكرّر أنك فاسد عظيم، بل شيطان وشرير. أنت لا تستطيع أن تؤمن بالله... من الواضح أنك لا تؤمن بأي مبدأ أخلاقي شخصي... كينغ: هنالك شيء وحيد تبقى لك كي تفعله. أنت تعرفه جيّداً. بقي لديك 34 يوماً لتفعل ذلك. (جرى اختيار الرقم لسبب محدّد، هو أنّ له دلالة عمليّة). أنت انتهيت. لم يتبق لك سوى طريق وحيد للخلاص. من الأفضل لك اعتماد ذلك الخيار، قبل أن تتعرّى نفسك الفاسدة وغير الطبيعيّة أمام الأمة».

• في مايلي الكلمات التي استعملها الكونغرس في وصفه لبرنامج «كوييتلبرو» الذي استخدمته الـ «إف بي آي» في الرقابة عام 1976⁽¹⁰⁰⁾: «فيما تمثّل الهدف المُعلن من تلك البرامج في حماية «الأمن القومي» أو منع العنف، يقرّ الـ «إف بي آي» بأنّ معظم أهدافها كانوا أشخاصاً مسالمين غير عنيفين، ولم تكن لهم صلة بقوة أجنبيّة. بالطبع، جرى استهداف أشخاص ومنظمات سلميّة من قِبَل الـ «إف بي آي»؛ لأنها حسبت أن لديهم ميلاً «كامناً» للعنف؛ وأما المواطنون غير العنيفين الذين عارضوا الحرب في فيتنام، فاستهدفهم الـ «إف بي آي» لأنهم يقدّمون «الدعم والأمان» للمتظاهرين العنيفين، بإعطاء الاحترام لقضيتهم... لكن برنامج «كوييتلبرو» لم يكتف ببساطة بمجرد اختراق الدستور والقانون. ففي سياق برنامج

(*) أُطلّقت تلك التسمية على حركة سلمية نادت بالمساواة في الحقوق بين السود والبيض، في ستينيات القرن العشرين، وكان القس الإفريقي - الأميركي مارتن لوثر كينغ أبرز قادتها.

«كوييتلبرو»، وضعت الـ «إف بي آي» يدها على القانون، وذهبت إلى أبعد من جمع المعلومات، وتخطت المهمة الموكلة لها بدعم إنفاذ القانون؛ فعملت خارج العملية القانونية برمتها؛ وعلمت سرّاً على إقلاق مواطنين ومجموعات ومضايقتهم وضرب مصداقيتهم.

لم يتغيّر شيء. وبعد 9/11 تجسّست الولايات المتحدة على «حركة احتلوا وول ستريت»⁽¹⁰¹⁾، ونشطاء الدفاع عن الحق في الإجهاض ورافضيه أيضاً⁽¹⁰²⁾، ونشطاء السلام⁽¹⁰³⁾، ومحتجين سياسيين آخرين⁽¹⁰⁴⁾.

• تجسّس الـ «إف بي آي» و«وكالة الأمن القومي» على أميركيتين مسلمين بارزين لا صلة لهم مع الإرهاب⁽¹⁰⁵⁾، ومن ضمنهم: فيصل جيل (نشط لأوقات طويلة في صفوف الحزب الجمهوري، وترشّح لمنصب عام، وكان لديهم تفويض أمني مرتفع المستوى)، وعاصم غفور (وهو محام بارز تولى تمثيل أشخاص في قضايا متّصلة بالإرهاب)، وهوشانك أمير أحمددي (بروفسور في العلاقات الدوليّة من «جامعة روتغرز»)، ونهاد عوض (المدير التنفيذي لأكبر منظمة للدفاع عن حقوق الأميركيين- المسلمين في الولايات المتحدة).

• تحت غطاء السرية، تسلسل بوليس نيويورك إلى أحياء الأقليات⁽¹⁰⁶⁾. وراقب مساجد، واخترق مجموعات طلابيّة وسياسيّة، وتجسّس على شرائح مجتمعيّة بأسرها. وكرة أخرى، استُهدف أميركيون بسبب انتمائهم إلى هويّة إثنيّة محدّدة، وليس لإدانتهم بجرائم ولا بأفعال خارجة عن القانون. نفّذ كثيرٌ من تلك العمليات بمعونة من الـ «سي آي إيه» على الرغم من أن القانون يحظر عليها التجسّس على أميركيتين.

هنالك المزيد من تلك الشواهد، إذ تجسّس «مركز الانصهار» في بوسطن على «ناشطين من أجل السلام»⁽¹⁰⁷⁾، والمنظمة النسوية المناهضة للحرب «كود بينك» (Code Pink) وحركة «احتلوا وول ستريت». في 2013، تعاونت مدينة بوسطن مع شركة «آي بي أم» في نشر مجموعة من كاميرات الفيديو لرقابة مهرجان موسيقي⁽¹⁰⁸⁾. في تلك الفترة عينها، تجسّست وحدة «النشاط على الأرض لمكافحة التجسس» التابعة للبتاغون على مجموعة من الأميركيين الأبرياء، وهو أمر يحظره القانون على وزارة الدفاع الأميركية⁽¹⁰⁹⁾.

وفي عمل يذكر بمحاولة هوفر استفزاز القسّ مارتن لوثر كينغ، عملت «وكالة الأمن القومي» على تتبع أنماط مشاهدةشرطة الجنس الإباحي لدى مجموعة من الأميركيين- المسلمين، ممن يعملون على «تحويل» الناس باتجاه تبني أفكار متطرّفة⁽¹¹⁰⁾، وهؤلاء ليسوا إرهابيين، لكنهم يستخدمون خطاباً سياسياً لدفع الآخرين صوب التطرّف. وكانت الفكرة من تلك الرقابة هي ابتزاز تلك المجموعة.

في 2010، فتّشت «وكالة مكافحة المخدرات» محتويات الخلوي لامرأة من مقاطعة «آلبيني»، بعد الحصول على إذن قانوني. لكن الوكالة احتفظت بالصور الحميمية التي عثرت عليها كي تصنع صفحة مزيفة باسم تلك المرأة على «فيسبوك»⁽¹¹¹⁾. وعندما مثلت الوكالة أمام القضاء، توسّعت الوكالة في استخدام حجة مفادها أن موافقة تلك المرأة على تفتيش هاتفها يحمل موافقة ضمنية على الاستيلاء على هويتها.

وتسيء السلطات المحليّة أيضاً استخدام قدرات الرقابة. في 2009، أعارت «مدرسة مقاطعة ماريون السفلى» مجموعة من أجهزة الـ «لاب توب» إلى طلبة في المرحلة الثانوية العليا، بهدف مساعدتهم في إنجاز فروضهم. وزرع مدرء المدرسة برامج تجسّس في تلك الحواسيب⁽¹¹²⁾، فسجّلت دردشات التلامذة مع بعضهم بعضاً، ورصدت مواقع الإنترنت التي زاروها، بل إنها- ولعل تلك أكثرها إثارة

للتقزز- صوّرتهم خلسة في غرف نومهم. وبرزت تلك القضية إلى العلن عندما واجه مساعد مدير المدرسة الطالب بلايك روبنز بصور تظهره وهو يتعاطى حبوباً مهلوسة متخفية بهيئة حبوب للحلوى. وبالتدقيق، تبين أنها حلوى من نوعين شهيرين في أميركا، وأدينّت المدرسة بسبب تلك الممارسات الاعتدائية المسيئة.

إضافة إلى إساءة استخدام السلطة بشكل واضح، هناك التوسع الحتمي للسلطة الذي يرافق كل نظام بيروقراطي واسع وقوي. ويشار إلى ذلك بمصطلح «زحف المهمة». ومثلاً، بعد 9/11، تآزرت جهود الـ «سي آي إيه» مع وزارة الخزانة، في جمع بيانات عن معاملات مالية لأمركتيين؛ سعياً لتقصي التمويل المحتمل للجماعات إرهابية مستقبلاً. وعلى الرغم من ذلك تبين أنه هدف غير واقعي⁽¹¹³⁾، إلا أن الجهود نجحت في اكتشاف بعض ممارسي تبييض الأموال، ما جعلها تستمر.

في الولايات المتحدة، تستخدم الرقابة بوتيرة أعلى⁽¹¹⁴⁾، وتطبق على حالات تتكاثر باستمرار، وتستعمل في تهم تتوسع دائرتها باطّراد؛ بل إن ذلك بات يجري أكثر من أي وقت مضى. أُعطيت سلطات الرقابة سنداً قانونياً في «قانون باتريوت» بوصفها شأنًا أساسياً في مكافحة الإرهاب، وكذلك بالنسبة لمذكرات التفتيش من النوع المعروف باسم «تسلّل وتلصّص»؛ وكلاهما بات شائعاً استخدامهما خارج إطار مكافحة الإرهاب، كعمليات التفتيش عن المخدرات. في 2011، حوّلت «وكالة الأمن القومي» سلطة الرقابة على مهربي المخدرات، إضافة إلى المشاغل التقليدية للأمن القومي⁽¹¹⁵⁾. وصدرت توجيهات إلى موظفي «وكالة مكافحة المخدرات» بأن يكذبوا في المحاكم؛ بهدف إخفاء أن «وكالة الأمن القومي» كانت تمرّر معلومات إليهم⁽¹¹⁶⁾.

هنالك ما تطلق «وكالة الأمن القومي» عليه تسمية «البنية الموازية»⁽¹¹⁷⁾. ويقصد من ذلك أن المؤسسات التي تتلقى معلومات من الوكالة، يجب عليها أن تصطنع سُبلاً أخرى يمكن الإشارة إليها علانية بوصفها مصدراً للمعلومات. الأرجح

أن الوكالة أمّدت الـ «إف بي آي» بالمعلومات التي سمحت للأخيرة بإلقاء القبض على قرصان الكمبيوتر روس أولبريشت، المعروف باسم «دريد بايرت روبرتس»، الذي أدار موقعاً شبكياً اسمه «طريق الحرير» من دون أن يعرف عن هويته، يهدف إلى تمكين الناس من شراء المخدرات وغيرها من المواد الممنوعة⁽¹¹⁸⁾.

وتُلاحظ ظاهرة «زحف المهمة» أيضاً في المملكة المتحدة التي تستغل فيها الرقابة المختصة باقتلاع الإرهابيين⁽¹¹⁹⁾، في العمل ضد أشخاص يهربون التبغ، أو يزورون العناوين أو لا يهتمون بتنظيف مخلفات كلابهم وغيرها من التجاوزات اليومية البسيطة⁽¹²⁰⁾. إذ تمتلك البلاد كميات كبيرة من كاميرات الرقابة، ما يجعل «منطقياً» استعمالها بأكثر الطرق تنوعاً.

هناك أمثلة كثيرة تأتي من بلدان مختلفة. مثلاً، تجمع إسرائيل معلومات عن فلسطينيين أبرياء بغرض اضطهادهم سياسياً⁽¹²¹⁾. وفي ظل الوسائل التقنية للرقابة، يسهل الادّعاء بانزلاق الناس والمنظمات إلى وضع إساءة الاستخدام. بديهي القول إن الحكومات الأقل شرعية تلجأ إلى الرقابة كجزء من تصرفاتها، في ظل غياب الحماية القانونية لمواطنيها.

إنّها أشياء مهمّة حقّاً، حتى لو كنت ممن يثقون بالحكومة المتقلّدة للسلطة حاضراً. إذ يعتمد النظام المتّسم بالقوة على المصادقية الكاملة لكل شخص في السلطة⁽¹²²⁾؛ ما يعني أن معظم الأشياء تسلك مساراً صحيحاً وأنها تخفض من الإساءة المؤثرة للسلطة. يبقى هناك تفاحات فاسدة دوماً، فيكون السؤال فعلياً هو عن مدى الضرر الذي يُسمَح لها بأن تُحدثه بما تملكه من قوّة، إضافة إلى مدى فساد بقية الصندوق بأكمله. يفترض بالضوابط أن تعمل بكفاءة، سواء أكنّا متوافقين مع الحزب الحاكم أم لا.

تقليص حرية الإنترنت

في 2010، أَلقت وزيرة خارجية أميركا آنذاك السيّد هيلاري كلينتون خطاباً أعلنت فيه أنّ حرّية الإنترنت هدف رئيس في السياسة الخارجيّة لأميركا⁽¹²³⁾. ولبلوغ تلك الغاية، تمّول وزارة الخارجيّة وتدعم مجموعة من البرامج العالميّة⁽¹²⁴⁾، وتعمل على محاربة حجب الإنترنت، وتعزّز التشفير، وتعزّز إخفاء الهوية. وتهدف تلك الأشياء كلها إلى «تمكين كل طفل يولد في أي مكان في العالم، من الوصول إلى الإنترنت العالميّة بوصفها منصّة مفتوحة تتيح حرية الإبداع والتعلّم والتنظيم والتعبير عن الذات، من دون حجب ولا تدخل غير مناسب». لقد نُسِفَت تلك الأجندة عندما تبين بغرابة أن الولايات المتّحدة وغيرها من الحكومات الديمقراطية، مارست رقابة على الإنترنت من النوع نفسه الذي تنتقد ممارسته في البلدان الأكثر قمعيّة.

واغتنمت تلك البلدان القمعية الفرصة السانحة للتذرّع بالرقابة الأميركية في تبرير سياساتها الجائرة تجاه الإنترنت: رقابة أشد، حجباً أعتى ومزيداً من الانعزاليّة؛ وكلها توصل إلى إعطاء كل من تلك البلدان سيطرة أشد صرامة على ما يقوله مواطنوها أو يفعلونه. ومثلاً، إحدى ذرائع الحكومة المصريّة لخططها بشأن فرض رقابة على الـ «سوشال ميديا»، هو القول إن «أميركا تنصّت على المكالمات الهاتفية، وتتعبق كل شخص يسعى إلى النيل من أمنها القومي»⁽¹²⁵⁾. ويخشى الهنود أن تستخدم حكومتهم أفعال الولايات المتّحدة لتبرير الرقابة في الهند⁽¹²⁶⁾. ونذرت الصين وروسيا علانية بالنفاق الأميركي⁽¹²⁷⁾.

ويؤثّر ذلك في حرّية الإنترنت عالمياً. تاريخياً، أُسِنِدَت حوكمة الإنترنت - بغض النظر عن ضآلتها أصلاً - إلى الولايات المتّحدة؛ لأن الجميع يعتقد بأن الأميركيّين يعملون لمصلحة حرية الإنترنت، وليس بالضد منها. وأما حاضراً، بعد أن فقدت الولايات المتّحدة كثيراً من مصداقيتها، دخلت حوكمة الإنترنت في مرحلة

الاضطراب. وتسعى مؤسسات تشريعية مؤثرة في الإنترنت إلى صوغ تصوّر عن نوع القيادة الملائم لتلك الشبكة. وتحاول المنظّمات المعيارية الدولية القديمة أن تؤثر في حوكمة الإنترنت بتطوير مجموعات من القوانين القومية لتلك الشبكة.

يمكن اعتبار ذلك بوصفه حراكاً باتجاه السيادة الإقليمية - القومية على الإنترنت، ويهدّد بتفتيتها. ليس ذلك بالأمر الجديد، لكنه لقي دفعاً هائلاً مع الكشوفات بصدد تجسّس «وكالة الأمن القومي» على الإنترنت. تجهد دول كروسيا والصين والمملكة العربية السعودية، في الدفع باتجاه زيادة السيطرة المستقلة على أجزاء الإنترنت التي تمر في أراضيها.

في حال تحقّق ذلك، تكون كارثة. في أساس الإنترنت أنها منصّة عالمية. وفي ما تستمر البلدان في الرقابة والحجب، ما زال بإمكان الشعب في البلدان القمعية أن يقرأ مزيداً من المعلومات وأن يتبادل الأفكار مع بقية شعوب العالم. تمثّل حرية الإنترنت قضية لحقوق الإنسان، وهي جديرة بأن تلاقى دعماً من الولايات المتحدة. وعلائية، حضّ مؤسّس «فيسبوك» مارك زوكربيرغ إدارة أوباما على ذلك، وكتب: «يجدر بحكومة الولايات المتحدة أن تكون البطل في الدفاع عن الإنترنت، لا أن تكون تهديداً لتلك الشبكة»⁽¹²⁸⁾. إنّه محقّ تماماً.

8

العدالة التجارية والمساواة

عملت مؤسسة «أكريتف هيلث» (Accretive Health) المختصة في تحصيل الديون، لدى عدد من المستشفيات في ولاية «مينسوتا»⁽¹⁾. وتولّت مسؤولية الفواتير وتحصيلها في تلك المستشفيات، إضافة إلى وضع جداول العمل، وترتيبات إدخال المرضى، وخطط الرعاية الصحية، وتحديد مدد بقاء المرضى في المستشفى. إذا بدا أن المسألة فيها تضارب في المصالح، فالأرجح أنها كانت كذلك. تولّت الوكالة أيضاً جمع معلومات موسّعة عن المرضى ووضعها في خدمة غاياتها الخاصة، دون أن تفصح للمرضى عن طبيعة مسؤوليتها في الرعاية الصحية المقدّمة لهم، إذ استخدمت معلوماتها عن ديون المرضى في ترتيب خطط علاجهم، وضغطت على المرضى في غرف الطوارئ للحصول على الأموال. أنكرت الوكالة أنها أساءت التصرف، لكن العام 2012 شهد تسوية قضائية في «مينسوتا» فرضت إبعاد الشركة عن تلك الولاية لما يتراوح بين ستين و6 سنوات⁽²⁾. من ناحية، يدل ضبط «أكريتف هيلث» متلبّسة بأخطائها ثم توقيع عقوبة قضائية عليها إلى أن النظام يعمل بشكل جيّد. من ناحية ثانية، تدل تلك القضية على سهولة إساءة استخدام المعلومات عنا.

تشهد قصص مماثلة لما حدث مع «أكريتف هيلث» على وجود خطر فعلياً على المجتمع من السماح للشركات بالرقابة العامة؛ إذ تساهم الرقابة الواسعة التي تنهض بها الشركات في الإساءات التي توجّه إلى الحريات المدنية، والتقدّم الاجتماعي

والحرية؛ وفق ما سبق أن وصفته في الفصل السابق. وإضافة إلى مساهمتها في الرقابة الحكومية، تحمل رقابة الشركات مخاطرهما الخاصة أيضاً.

التمييز المستند إلى الرقابة

بطريقة أساسية تماماً، تستخدم الشركات بيانات الرقابة في التمييز⁽³⁾، إذ تصنف الناس ضمن فئات مختلفة، وتسوّق السلع والخدمات إليهم بطرق متميزة، استناداً إلى معلومات الرقابة.

في ستينيات القرن العشرين، استخدم تعبير «بواسطة الخطوط الحمر»⁽⁴⁾ لوصف ممارسة تمييزية قديمة: تعتمد البنوك ممارسة التمييز ضد أفراد الأقليات الإثنية لدى محاولتهم شراء منازل. لم تكن البنوك لتوافق على إعطاء رهونات عقارية في مناطق قريبة من أحياء الأقليات - لذا كانت ترسم خطوطاً حمراً على خرائط البنوك لإظهار تلك المناطق. وكذلك كانت البنوك لا توافق على رهونات عقارية لأفراد الأقليات إلا إذا كانوا بصدد شراء منازل في أحياء تقطنها غالبية من الأقلية التي ينتمون إليها. بالطبع، لم يكن ذلك شرعياً، لكن البنوك مارسته لفترة طويلة من دون أن تعاقب عليه. وبصورة أكثر تعميماً، يمكن القول: ممارسة رسم الخطوط الحمر تعني الإمساك عن تقديم خدمات [أو تقديمها بأسعار مبالغ فيها] مع استخدام مكان السكن كاسم آخر للعرق - وهو أمر تزيد سهولته كثيراً باستخدام الإنترنت⁽⁵⁾.

في العام 2000، أنشأ بنك «ويلز فارغو» موقعاً إلكترونياً للترويج لعروضاته في الرهونات العقارية⁽⁶⁾. وقدّم الموقع «آلة حاسبة مجتمعية» لمساعدة الشراء المحتملين في التعرف إلى الأحياء التي يحتمل أن يقطنوها. وتحسب تلك الآلة أرقام البلدية الحاضرة للشراء المحتملين، وترشدتهم إلى أحياء تنسجم مع العرق المهيمن في الأحياء التي تدل عليها أرقام البلدية الحالية للساعين إلى الشراء. بمعنى آخر، عمل الموقع على إرشاد المشتريين الآتين من أحياء تسكنها غالبية من البيض إلى منازل في أحياء مماثلة، وكذلك الحال بالنسبة لأصحاب البشرة السمراء.

تسمى تلك الممارسة بواسطة «خطوط الويب»⁽⁷⁾، وتملك قدرة كامنة على ممارسة التمييز بطرق أشد وأكثر توسعاً من سياسة «بواسطة الخطوط الحمر» التقليدية. ولأن الشركات تجمع معلومات وافرة جداً عنّا، وتستطيع وضع ملفّات عن صفاتنا الشخصية؛ لذا تتمكن من التأثير فينا بطرق متنوّعة. وفي 2014، خلص تقرير صادر عن البيت الأبيض بشأن «البيانات الضخمة» إلى القول إنّ «الأدوات التحليلية في البيانات الضخمة تملك القدرة على الإضرار بكل أنواع الحماية للحقوق المدنية، المتعلقة بطُرق استخدام المعلومات الشخصية في الإسكان والإقراض والتوظيف والصحة والتعليم والسوق»⁽⁸⁾. أميل للاعتقاد بأن التقرير تفهّم خطورة «البيانات الضخمة».

يشكّل التمييز في الأسعار شيئاً فائق الأهمية حاضراً. إذ يتجاوز التمييز التقليدي في العرق ونوع الجنس مثلما يحصل في «بواسطة خطوط الويب»؛ لأنه يتضمن أن تعطي الشركات أسعاراً متفاوتة لفتات مختلفة من الناس كي تحصل على أقصى قدر من الأرباح. باتت تلك الممارسة شبه مألوفة في حجوزات الطيران. إذ تتغيّر الأسعار باستمرار اعتماداً على عناصر من نوع كم ندفع مقدّماً، في أي الأيام نسافر ودرجة امتلاء الطائرة بالركاب.

تهدف شركات الطيران من تلك الممارسة إلى بيع تذاكر السفر بأسعار تفضيلية إلى من يقضون إجازاتهم في الخارج ما يجعل هؤلاء يقبلون شراءها. في المقابل، تستخرج من المسافرين لإنجاز الأعمال أرباحاً أعلى طالما أنهم يقبلون دفعها. لا يوجد ما هو شيطاني في تلك الممارسة باعتبار أنها تتعلّق بمضاعفة العائدات والأرباح. وعلى الرغم من ذلك، لا يجوز التمييز في الأسعار شعبية كبيرة عند الناس. ومثلاً، يوصف رفع سعر مجارف الثلج بعد عاصفة ثلجية بأنّه تسعير ابتزازي. ولذا، يجري تمويهه ضمن عروض خاصة، أو منح كوبونات أو بطاقات استرجاع المال.

هناك أنواع غير قانونية من التمييز بالأسعار. ومثلاً، لا يستطيع المطعم أن يبارس تمييزاً بالأسعار استناداً إلى العرق أو النوع الجنسي للزبون. في المقابل، يستطيع وضع أسعار تتغير وفق أوقات تناول الطعام، وهو سبب وضع أسعار مختلفة لوجبتي الغداء والعشاء على الرغم من احتوائهما الأطباق عينها. ويعتبر أمراً قانونياً أن تعطى أسعار وجبات تفضيلية للمسنين، وكذلك الحال بالنسبة لوجبات الأطفال. ويندرج ضمن الممارسة القانونية فرض شركة «أوبر» أسعاراً أعلى لتوصيلاتها في أوقات الذروة في حركة المواصلات⁽⁹⁾.

في أعمال كثيرة، تُقدّم لك عروض، وتُمنح لك أسعار وتحصل على خدمات، استناداً إلى المعلومات عنك. يشمل ذلك قروض البنوك، التأمين على السيارة، بطاقات الائتمان وما إلى ذلك. تسهل رقابة الإنترنت الضبط الدقيق لتلك الممارسة. وصار سائداً على الشبكة أن يعرض الباعة الإلكترونيون عليك أسعاراً وخيارات متنوّعة، استناداً إلى تاريخك وما يعرفونه عنك⁽¹⁰⁾. واعتماداً على من تكون⁽¹¹⁾، ربما ترى صورة لسيارة همراء بسقف متحرك أو سيارة عائليّة من نوع «ميني - فان» في ما يصلك من إعلانات السيارات، وكذلك تعطى خيارات مختلفة في سداد الثمن والتخفيضات، عند زيارتك لموقع موزع السيارات. ووفق مقال ظهر في صحيفة وول ستريت جورنال (Wall Street Journal) في 2010، فإن الأسعار التي يعرضها عليك موقع «ستابلز» للشراء الإلكتروني بالمفرّق، تعتمد على مكان سكنك، ومدى قرب محل منافس من منزلك. ويورد المقال عينة أن شركات كبرى للمبيعات كـ «روزيتا ستون» و «هوم ديو»، تمارس أيضاً سياسة تغيير الأسعار وفقاً للمعلومات الفردية عن المستهلك⁽¹²⁾.

وبصورة أوسع، لكل مناسجه كزبون⁽¹³⁾. ويربط سيطرة المعلومات ذلك الملف بكل واحد منا. ويشبه السجلّ جداول بطاقات الائتمان، لكنه لا يتألف من عنصر مفرد [كالمال في تلك البطاقات]، بل يركّز على ما تشتريه استناداً إلى أشياء كالبيانات عما اشتريته من مخازن البيع بالتجزئة، المعلومات عن وضعك المالي، البيانات الآتية

من استطلاعات الرأي، وبيانات تسجيل بطاقات ضمان السلع، التفاعلات المختلفة بواسطة الـ «سوشال ميديا»، وبيانات بطاقات ولاء المستهلك، السجلات العامة، تفاعلاتك مع مواقع الإنترنت، قوائم الأعمال الخيرية، اشتراكاتك على الـ «ويب» وخارجه أيضاً، والبيانات عن صحتك ولياقتك. وتستعمل تلك المعلومات كلها لتحديد نوع الإعلانات والعروض التي ستشاهدها أثناء تجوالك في الإنترنت.

في العام 2011، كوّن الجيش الأميركي مجموعة من إعلانات التطوع، تُظهر جنوداً من إثنيات وهويات جنسية مختلفة⁽¹⁴⁾. وتشارك مع إحدى شركات الكابل في توزيع تلك الإعلانات بما يتوافق مع المعلومات الديموغرافية عن يسكن كل منزل على حدة.

هنالك طُرُق أخرى في التمييز. في 2012، وضع فندق «أوريتز» أسعاراً متباينة لغرفة، تميز بين النزلاء الذين يستخدمون نظام «ويندوز» وأولئك الذين يستعملون نظام الـ «ماك»⁽¹⁵⁾. وتتصدّد مجموعة من المواقع الشبكية للسفر والسياحة إظهار صفقات مختلفة لزوّارها؛ استناداً إلى تاريخ التصفح لكل زبون⁽¹⁶⁾. وتستند بعض المواقع إلى معرفتها بالمستوى الاقتصادي لزوّارها، فتظهر لهم صفحات تتوافق مع مستوى دخلهم. يبدو كثير من تلك الأشياء مرهفاً تماماً. إذ لا تعني تلك الممارسات أنك لن تشاهد أسعار رحلات سياحية أو غرفاً فندقية معينة، بل أن يضع الموقع ترتيباً لتسلسل ظهور صفحاته بما يتفق مع معلوماته عن زائريه، مع افتراض أن الزبون يختار الأكثر سهولة بالنسبة له. وفي الفصل 3، رأينا أنّ بياناتنا يمكن استعمالها لمعرفة العمر والنوع والخيار الجنسي، وحال العلاقات الخاصة وأشياء كثيرة أخرى. يعطي ذلك الوضع للشركات اليد العليا على حساب جمهور المستهلكين، ومع استمرار الشركات في مراكمة المعلومات عن الأفراد والطبقات؛ تتزايد سيطرتها وتتقوى بآطراد. ومثلاً، يعلم المسوّقون أن المرأة تمحّس بأن جاذبيتها تكون أقل يوم الاثنين باعتباره بداية أسبوع العمل، فترى الشركات فيه اليوم المناسب لإمطارهن بإعلانات عن مواد التجميل⁽¹⁷⁾. وكذلك تعلم الشركات أن ردود الفعل على

إعلاناتها تتفاوت وفق العمر ونوع الجنس⁽¹⁸⁾. ومستقبلاً، ربما أصبحت معلومات الشركات عن الأفراد أكثر دقة، ما يزيد من دقتها في توجيه إعلاناتها. إذا علمت الشركات أنك في الثامنة صباحاً تكون مشوشاً لأنك لم تتناول قهوتك، تتجنب إرسال إعلاناتها إليك في تلك الساعة. وتنطلق إعلاناتها إليك في التاسعة والنصف، بعد أن تفعل القهوة فعلها، ثم تتجنبك بعد الساعة 11 نهاراً؛ لأن شيئاً من التشوش يعود إليك مع انخفاض مستوى السكر في دمك قبيل موعد الغذاء.

وكذلك يجري الحكم على الناس وفقاً لشبكة علاقاتهم على الـ «سوشال ميديا». تعمل شركة «ليندو» الفلبينية على تقييم صلاحية الأفراد للقروض، بتدقيق الوضعية المالية لمن يتفاعلون معهم باستمرار على «فيسبوك»⁽¹⁹⁾. وفي مثل آخر على التمييز «بواسطة خطوط الويب»، تخفض شركة «أميركان إكسبرس» سقف بطاقات الائتمان وفقاً لنوع المتاجر التي يتسوق منها طالب البطاقة⁽²⁰⁾.

قدّم البروفسور أوسكار غندي، وهو أستاذ قانون في «جامعة بنسلفانيا»، وصفاً مبكراً عن ذلك الوضع برمته، إذ سمّاه في 1993 «الفرز بالرؤية الشاملة»⁽²¹⁾، مشيراً إلى «عمليات تجميع المعلومات وتحليلها ومشاركتها، وهي تشمل الأفراد والمجموعات. ويجري توليد تلك المعلومات في سياق الحياة اليومية للناس بوصفهم مواطنين وموظفين ومستهلكين. وتستخدم المعلومات في السيطرة على مدى وصولهم إلى البضائع والخدمات التي تحدّد الحياة في الاقتصاد الرأسمالي المعاصر». من المؤكّد أن من يملكون ذلك النوع من السلطة، يمتلكون سلطة ضخمة فعلياً. إنها سلطة استعمال مؤشرات تمييزية لتوزيع الفرص والوصول والاستحقاق والأسعار⁽²²⁾ (غالباً ما تكون على هيئة عروض خاصة وتخفيضات) والاهتمام (إيجابياً وسلبياً) والتعرّض للمعرفة.

من المحتمل أن تغدو تلك الممارسة تدخلية جداً، إذ شرعت المطاعم الفاخرة في التفتيش عن معلومات عن أسماء زبائنهم بواسطة «غوغل»؛ بهدف تحسين تجربة

تناول الطعام فيها⁽²³⁾. إنها لا تستطيع أن تعطي الوجبات نفسها بأسعار متفاوتة، لكنها تقدر أن تقدّم قائمتها للمشروبات الروحية أنواعاً باذخة أو رخيصة. وتجرب شركات تأمين المركبات يدها في ربط التأمين بأداء الزبون على الطرقات. إذا سمحت لشركة التأمين أن تعرف أوقات قيادتك لمركبتك، والمسافات التي تقطعها، وسرعتك في القيادة؛ فلربما حصلت على تأمين بأقساط أرخص⁽²⁴⁾.

تزيد إمكانات التدخل بصورة كبيرة في إطار علاقة الموظف برب العمل. ثمة شركة واحدة على الأقل فاوضت على إمكان توزيع سوارات «فت بت» الرقمية التي تقيس مؤشرات الصحة الجسدية على موظفيها، مع إعطاء شركات التأمين الصحي معرفة غير مسبقة تاريخياً عن العادات الصحية للزبائن بسوارات «فت بت»⁽²⁵⁾. وعلى نحو مماثل، تفرض ثانويات كثيرة على طلبتها ارتداء مجسات ذكية لقياس دقات قلوبهم أثناء ممارسة الرياضة، لكنها لا تنطق ببنت شفة عن طريقة استخدام تلك البيانات بعد تجميعها⁽²⁶⁾. في 2011، حلّت شركة «هيوليت باكارد» الشهيرة في صناعة الكمبيوتر بيانات موظفيها كي تعرف من موشك على تركها، ثم لفتت أنظار المدراء إليهم⁽²⁷⁾.

تشكّل الرقابة في مواقع العمل حقلاً جديداً محمّلاً بإمكانات ضخمة في الأذى⁽²⁸⁾. بالنسبة للعديد منّا، يعدُّ رب عملنا هو السلطة الأكثر خطورة في مراقبتنا⁽²⁹⁾. وتشمل قائمة الموظفين المعرضين للرقابة المنتظمة، موظفي مراكز المكالمات الهاتفية، سائقي الشاحنات، عمال الصناعة، طواقم المبيعات، عمال البيع بالتجزئة، وغيرهم. وتزايد أعداد من يتعرّضون لرقابة إلكترونية مستمرة، من قبل الشركات التي يعملون فيها. تأتي معظم تلك الأشياء من حقل جديد يسمّى «تحليلات موقع العمل»، وهي أساساً إدارة الموارد البشرية استناداً إلى معلومات الرقابة⁽³⁰⁾. إذا استعملت الاتصالات الإلكترونية للشركة كالحاسوب والخلوي، فأنت تعطي مديرك الحق في معرفة كل ما تفعله على تلك الأجهزة⁽³¹⁾. يمتلك بعض تلك الممارسات شرعية، فمن حق رب العمل أن يضمن أنك لا تمارس لعبة

«فارم فيل» (Farmville) الشهيرة طيلة اليوم. لكنك ربما استخدمت تلك الأجهزة في أوقاتك الخاصة، لإنجاز اتصالات بعضها خاص والآخر متصل بالعمل.

كلما تعرّضنا للرقابة والتصنيف المستند إليها، تزايد إمكان أن تسير الأمور في مسار الخطأ. هناك مثل صار مألوفاً لديك: فكّر بكل تلك الإعلانات الفائضة التي تندفق إليك بواسطة الإنترنت مستندة إلى تحليلات حسابية ربما تسيء التعرف إلى اهتماماتك. يتقبّل بعض الناس ذلك، فيما يمثل لآخرين أذية نفسية منخفضة المستوى، تتأتى من استعمال البيانات لتصنيفهم ووضعهم في فئات، سواء عن حق أم باطل⁽³²⁾. ويتزايد إمكان حدوث الأذى كلما كان الحكم على الشخص له أهمية أكبر، كأن يصنّف الأفراد في فئات بالنسبة للقروض الائتمانية استناداً إلى أرقام وجداول خوارزمية، وكذلك تعتمد طريقة تعامل قوى الأمن معنا في المطارات على المعلومات التي جمعتها الشركات عنا، ولو بصورة جزئية.

يترتب على ذلك الوضع آثارٌ مفرّعة اجتماعياً. إذ يعزف الناس مثلاً عن التفتيش عن معلومات حول أمراضهم؛ خوفاً من وصول بيانات عمليات التفتيش على الإنترنت إلى شركات الضمان الصحي، ما يؤدي إلى إخراجهم من شبكة ذلك الضمان⁽³³⁾.

ويصح القول إنّ جزءاً كبيراً من التصنيف الذي تنهض به الشركات يبدأ بنوايا طيبة. فلربما حُرِمَ أناسٌ من قروض بنكية بسبب الإنهاك المالي لأصدقائهم على «فيسبوك»، لكن النظام الذي صنّعه شركة «ليندو» الفليبيّة [انظر أعلاه] يسمح بإقراض من ليس لهم تصنيف ائتماني: إذا كان لأصدقائهم وضع ائتماني جيد جيداً، يسجل ذلك كعلامة لصالحهم. وفي طيات استخدام المعلومات الشخصية في تحديد نسب التأمين أو سقف الائتمان المالي، أن بعض الأشخاص ربما حصلوا على صفقات أسوأ من تلك التي كان ممكناً أن ينالوها لولا المعلومات الشخصية عنهم، فيما يكون الوضع معكوساً بالنسبة لكثيرين أيضاً.

وبصورة عامة، تستعمل الشركات الكبرى بيانات الرقابة لزيادة أرباحها على حساب الزبائن⁽³⁴⁾. ولا يستسيغ الزبائن ذلك، ولكن طالما أن (1) الباعة يتنافسون بين بعضهم بعضاً للحصول على أموالنا، و(2) شركات المعلوماتية تصنع برامج تسهّل ممارسة الأسعار التمييزية، و(3) التمييز يجري خفية عن الزبائن؛ يكون من الصعب على الشركات مقاومة إغراء تلك الممارسة.

التلاعب استناداً إلى الرقابة

من يمتلك معلومات عنا يمتلك قدراً من التحكم بنا، ومن يعرف كل شيء عنا يمتلك قدرة كبيرة على التحكم بنا. باختصار، الرقابة تسهّل التحكم.

ليس ضرورياً أن يشمل التلاعب الإعلان المباشر. إذ يمكن أن يكون ترتيباً للمنتجات يجعلك ترى صوراً تظهر في خلفيتها سيارة من ماركة معينة. ولربما اقتصر أمره على الوتيرة التي ترى فيها تلك السيارة. وأساساً، يمثل ذلك نموذج العمل لدى محرّكات البحث على الإنترنت. وفي أزمانها الأولى، تداولت المحرّكات كلاماً عن إمكان أن يدفع المعلنون أكثر مقابل ظهورهم أولاً في نتائج عمليات التفتيش بتلك المحرّكات⁽³⁵⁾. وبعد احتجاج من الجمهور أودى إلى صدور توجيهات من «اللجنة الفيدرالية للتجارة»، لجأت محرّكات البحث إلى التمييز بصرياً بين النتائج التي تأتي «طبيعياً» من الجداول الخوارزمية، وتلك التي توضع في الصدارة لأنها مدفوعة⁽³⁶⁾. وحاضراً، تظهر النتائج المدفوعة في مربعات صفّر على محرّك «غوغل»، فيما يضعها محرّك «بينج» في مربعات ملوّنة بالأزرق الخفيف. وسرت الأمور كذلك لفترة معينة، ثم انتقلت الأمور إلى وضعها السابق في الآونة الأخيرة. إذ بات «غوغل» يتلقى أموالاً لقاء وضع روابط إلكترونية لمواقع معينة في مركز متقدّم من نتائج البحث، ولم يعد يكفي بوضعها في مساحة إعلانية منفصلة⁽³⁷⁾. لا نعلم المدى الذي ستذهب إليه الأمور، لكن «اللجنة الفيدرالية للتجارة» شرعت في الاهتمام به أيضاً⁽³⁸⁾.

عندما تقلّب المواد التي تصل إلى صفحتك على «فيسبوك»، فأنت لا تطالع كل تدوينة ومن كتبها؛ بالأحرى أنت تطالع المواد وفق ترتيب تعدّه في دواخل الموقع جداول خوارزمية مؤتمتة لا يُصار إلى كشفها للعموم. ولكن، تذكر أن هنالك من هم مستعدون لأن يدفعوا لقاء أن تكون تدويناتهم [«بوست»] أول ما يقرؤه الأصدقاء أو المعجبون على صفحاتهم. يشكّل ذلك النوع من الدفع مقابل التوضع شرطاً أساسياً من مداخل «فيسبوك»⁽³⁹⁾. وعلى غرار ذلك، فإن معظم الروابط الإلكترونية التي توصل إلى المقالات الإضافية في صفحة الأخبار، إنّما هي روابط دفع أصحابها لقاء ذلك التوضع.

هناك كثير من التلاعب كامن في ذلك السياق. إليك أحد النماذج. في الانتخابات الرئاسية للعام 2012، نال مستخدمو «فيسبوك» إمكان وضع أيقونة «أنا اقترعت»، تشبه كثيراً تلك اللصقة التي نحصل عليها بعد وضع الورقة في صناديق الاقتراع فعلياً. هنالك تأثير الالتحاق بالآخرين الذي أثبتته وثائق كثيرة، بمعنى أنك تميل أكثر إلى التصويت لدى معرفتك بأن أصدقاءك صوّتوا قبلك. أدى ذلك التلاعب إلى زيادة الإقبال على التصويت بمعدل 0.4٪ على مستوى الولايات المتحدة⁽⁴⁰⁾. لا شيء مؤذٍ في ذلك، عند هذه النقطة. لكن، تخيل لو تلاعب «فيسبوك» بأيقونة «أنا اقترعت» إما وفق الانتماء الحزبي، أو بعض بدائله المقبولة كأرقام المناطق البلدية للمنازل، أو نوع المدونات المفضلة أو الروابط الإلكترونية التي أبدى إعجابه بها وغيرها. لم يفعل «فيسبوك» ذلك، لكن لو أنّه فعل لتمكن من تغيير معدل التصويت لمصلحة تيار معين. وكذلك لكان من الصعب اكتشاف ذلك، بل إنه ربما لا يكون غير قانوني⁽⁴¹⁾. يستطيع «فيسبوك» أن يقلب اتجاه التصويت في انتخابات مقاربة النتائج، بالتلاعب بالأولوية التي يرى فيها الجمهور تدوينات الـ «بوست» على صفحاتهم⁽⁴²⁾. وربما يفعل «غوغل» أمراً مشابهاً بواسطة التلاعب بنتائج عمليات التفتيش عليه⁽⁴³⁾.

إذا عقدت إحدى المنصات السيئة النوايا في الـ «سوشال ميديا» عزمها على التلاعب بالرأي العام، فيمكنها أن تمضي أبعد مما سبق وصفه⁽⁴⁴⁾. إذ تستطيع تضخيم أصوات الناس الذين تتوافق معهم، وتمش من لا تتوافق معهم، ما يعطيها القدرة على تحريف مسار الجمهور. فعلت الصين ذلك بـ «حزب الخمسين بالمئة» (50 Cent Party)⁽⁴⁵⁾. وفي الصين، تستخدم التسمية في الإشارة إلى أشخاص استأجرتهم الحكومة لنشر تدوينات [«بوست»] مؤيدة للحزب الشيوعي الصيني على الشبكات الاجتماعية، وتحدي التعليقات المعارضة لمواقف ذلك الحزب. وانخرطت شركة «سامسونغ» في أمر مُشابه تماماً⁽⁴⁶⁾.

وفقاً للمفك الشخصي كمستخدم للإنترنت، تتلاعب شركات عدّة في ما تراه على الشبكة⁽⁴⁷⁾: عمليات البحث التي أجريتها على «غوغل»، والأخبار التي طالعها على «ياهو»، وحتى وتيرة مطالعتك لصحف كبرى مثل نيويورك تايمز. إنّه لأمر جليل. إذ تحصل الصفحة الأولى من نتائج البحث في «غوغل» على ثلث إجمالي المشاهدات⁽⁴⁸⁾؛ فإن لم تكن على الصفحة الأولى، فالأرجح أنّك غير موجود. وبالنتيجة، صارت الإنترنت التي تراها أكثر ميلاً لأن تكون مفضّلة على مقاس ملف ملاحك الشخصية مع ما يتضمّنه من مؤشرات على مصالحك⁽⁴⁹⁾.

ويقود ذلك إلى ظاهرة سمّاها الناشط السياسي الأميركي إيلي باريزر «فقاعة الفلتر»⁽⁵⁰⁾؛ بمعنى أن تصلك «إنترنت» تكون مفضّلة على مقاس خياراتك، فلا تطالع أبداً رأياً لا يتفق مع توجهاتك. ربما ظننت أن ذلك الأمر ليس سيئاً، لكنه مؤذٍ تماماً على المستوى الواسع⁽⁵¹⁾. إذ لا نرغب في العيش في مجتمع لا يقرأ فيه الجميع طيلة الوقت إلا الآراء التي تدعم آراءهم⁽⁵²⁾، وليس الحال فعلياً أننا لا نتعرّض أبداً لتلك المواجهات التي تجددنا وتوافقنا وتحدّنا وتعلّمنا.

في 2012، أجرى «فيسبوك» تجربة أبقاها تحت السيطرة⁽⁵³⁾. إذ تلاعب بالتدوينات التي تصل وتتجدّد على صفحات 680 ألف مستخدم، مُظهرًا لهم

تدوينات إما أكثر سعادة أو أشد تعاسة. ولأن «فيسبوك» يقيم مستخدميه باستمرار - وهي الطريقة التي يستخدمها في جعل جمهوره مورداً إعلانياً - كان من السهل عليه تقييم الأشخاص المشمولين بالتجربة، وتجميع النتائج. وتبين لـ «فيسبوك» أن الأشخاص الذين وصلتهم تدوينات سارة بوتيرة أعلى، كتبوا تدوينات أكثر سعادة، والعكس بالعكس. لا أرغب في المجادلة طويلاً بشأن تلك النتيجة. ولم تستمر تجربة «فيسبوك» إلا أسبوعاً وخلفت أثاراً ضئيلة. في المقابل، بمجرد أن تفهم مواقع كـ «فيسبوك» كيف تستطيع فعل ذلك بكفاءة، فسرعان ما ستحوّلها مصدراً للمال. لا تشعر النساء أنهن أقل جاذبية يوم الإثنين فحسب، بل يشعرن بذلك أيضاً عندما يكنّ مكتئبات⁽⁵⁴⁾. ونشهد حاضراً بدايات نُظُم تحلّل الصوت وحرركات الجسد كي تحدّد الحال المزاجية للشخص. وكذلك ترغب الشركات في معرفة متى يكون زبائننا أكثر إحساساً بالإحباط، ومتى يكون مجزياً زيادة عرض المبيعات لهم⁽⁵⁵⁾. ويشكّل التلاعب بالحال المزاجية بالتوافق مع منتجات السوق أمراً يرغب فيه عالم الإعلانات مهما بدا ذلك مرعباً بالنسبة لنا.

يغدو التلاعب أسهل بأثر من الطابع الممرّز لكثير من النُظُم التي نستخدمها. وتقف شركات كـ «غوغل» و«فيسبوك» في القلب من نُظُم اتّصالاتنا، ما يعطيها قوة كبرى في التلاعب والسيطرة⁽⁵⁶⁾.

هنالك أضرار فريدة من نوعها من الممكن أن تتأتى من استخدام بيانات الرقابة في السياسة. إذ تشبه إدارة الحملات الانتخابية تلك المتبعة في التسويق؛ كما شرع السياسيون في الاستفادة من القدرة الجديدة في الإعلان المشخص كأداة لتتبع أنماط التصويت المتمايزة، و«تسويق» مرشّح ما أو موقف سياسي معيّن. كذلك يستطيع المرشّحون ومجموعات المصالح الخاصة صنع إعلانات وحملات استجلاب الأموال مفصلة على قياس مجموعات معيّنة⁽⁵⁷⁾: من لديهم دخل يفوق 100 ألف دولار سنوياً، محبّذو اقتناء السلاح، الأفراد الذين قرأوا مقالات تعبر عن وجهة محدّدة في قضية ما، النشطاء المتقاعدون... بل كل ما يمكن أن تفكّر فيه. كذلك يستطيعون

توجيه إعلانات محملة بالغضب إلى مجموعة معينة، وإرسال إعلانات رزينة ومعمّقة سياسياً إلى مجموعات أخرى. ويتمكنون من المتابعة الدقيقة لحملات حثّ الناخبين على الاقتراع في يوم التصويت⁽⁵⁸⁾؛ وكذلك إعادة تقسيم المناطق الانتخابية بين اقتراع وآخر بما يتلاءم مع مصلحة حزب معين⁽⁵⁹⁾. تحمل تلك الأنماط من استعمال البيانات مخاطر أساسية على الديمقراطية والاقتراع⁽⁶⁰⁾.

وبطّراد، سوف تتحسن القدرة على التلاعب النفسي المستند إلى المعلومات الشخصية والتحكّم بالنظم التي تعتمد المعلومات عليها. وهناك ما هو أسوأ، يتمثّل في أن التلاعب النفسي سيرتقي إلى حدّ أننا لن نشعر به. ربما يصعب علينا قبول تلك الحقيقة؛ لأننا كلنا نؤمن بأننا أذكىء بدرجة تمنع من جعلنا ألعوبة بيد آخرين. حسناً: لسنا كذلك.

انتهاكات الخصوصية

في العام 1995، اخترق الـ «هاكر» كيفن ميتنيك شبكة تابعة لإحدى شركات الإنترنت، اسمها «نت كوم» (Netcom)، واختطف أرقام ما يزيد على 20 ألف بطاقة ائتمانية⁽⁶¹⁾. في 2004، اخترقت مجموعة من الـ «هاكرز» شبكة إحدى شركات سماسة المعلومات، اسمها «شويس بوينت» (Choice Point)، وسرقت بيانات ما يزيد على مئة ألف شخص، واستخدمتها في عمليات احتيال⁽⁶²⁾. في أواخر 2014، اخترق الـ «هاكرز» الشبكات الداخلية لمؤسسة «هوم ديو»، واستولوا على قرابة 60 مليون أرقام بطاقات ائتمانية⁽⁶³⁾، وبعدها بشهر؛ أعلن عن عملية سطو على معلومات ترجع إلى قرابة 83 مليون أسرة كانت لدى بنك «جي بي مورغان تشيس»⁽⁶⁴⁾. خلال عقدين من عمر الإنترنت، من الجلي أنه لم يتغيّر شيء سوى اتّساع مدى العمليات.

ثمة سؤال منطقي: إلى أي مدى تحمي شركات الإنترنت، وسماسة المعلومات والمؤسسات الحكومية؛ معلومات الجمهور؟ ومن وجهة معينة، يبدو السؤال ضئيل

الدلالة. ففي الولايات المتحدة، يستطيع أي شخص قادر على دفع المال مقابل الحصول على معلومات أن يفعل ذلك فعلياً. في بعض الأحيان، اشترى مجرمون بيانات بطريقة قانونية، ثم استخدموها في عمليات احتيال⁽⁶⁵⁾.

إن ظاهرة الجريمة السبرائية أقدم من الإنترنت نفسها، وتمثل أيضاً تجارة مربحة⁽⁶⁶⁾. وإذا يصعب الحصول على أرقام دقيقة، تسهل معرفة أنها تكلف الولايات المتحدة عشرات بلايين الدولارات. ومع أرقام كتلك، تكون الجريمة الإلكترونية الشبكية ظاهرة منظمة ودولية.

يتضمن شطر كبير من تلك الظاهرة سرقة الهوية، ما جعل الاحتيال بهوية متحلة أحد الخيالات الكبرى في عصر الإنترنت. إذ يخترق المجرم قاعدة بيانات في مكان ما، ويسطو على معلومات عن حسابك البنكي وربما كلمات المرور أيضاً، ويتحل شخصيتك للحصول على قرض باسمك. وربما سرق رقم بطاقتك الائتمانية واستخدمها في التبضع. ومن الممكن أن «يفرك» استرداد ضرائبي باسمك ويحصل على تلك الأموال، ما يعرضك للمساءلة القانونية لاحقاً⁽⁶⁷⁾.

ليست مسألة شخصية. إذ لا يركض المجرمون خلف معلوماتك الحميمة؛ بل جلّ ما يسعون إليه هو بيانات عن حساباتك المالية للوصول إليها. وكذلك يرومون بيانات شخصية تكفي للحصول على رصيدك.

قبل حفنة من السنين، كان الخطر الداهم يتمثل في إمكان أن يخترق المجرمون حاسوبك ويسطوا على معلوماتك وبياناتك. لكن مستوى سرقة البيانات استمر في الارتفاع مع الزمن. وفي أيامنا، بات المجرمون أكثر ميلاً لاختراق قواعد البيانات في الشركات الكبرى، ويسرقون معلوماتك الشخصية ضمن بيانات لملايين الناس. إنه أمر أكثر نجاعة. وكذلك تخترق قواعد البيانات الحكومية باستمرار⁽⁶⁸⁾. ومرة تلو الأخرى، تعلمنا أن بياناتنا لا تتمتع بحماية جيدة. تحدث سرقة البيانات بوتيرة منتظمة بأكثر مما يظهر في وسائل الإعلام. إذ يخبرني كثير من المحامين لشؤون

الخصوصية أن انتهاكات البيانات وهشاشاتها أكبر بكثير مما يعلن عنه - بل إن بعض الشركات لا تعي أن شبكاتهما اختُرِقت وبياناتها سُرقت⁽⁶⁹⁾. من المذهل معرفة مدى الرداءة في أمن الشركات. ولأن المؤسسات تحصل على بياناتك بطريقة شرعية، فإنها لا تتعرض للمساءلة إذا أضاعتها.

أحياناً، لا يسعى الـ «هاكرز» خلف الأموال. ففي العام 2010، اعتُقل مواطن من كاليفورنيا اسمه لويس ميهانغوس، بسبب «الابتزاز الجنسي»⁽⁷⁰⁾. وكان يخترق حواسيب ضحاياه من الإناث، ويبحث عن صورهن الجنسية، ثم يتسلل إلى كاميرا الكمبيوتر ليلتقط صوراً حميمة إضافية لهن. وبعدها، يتصل بهن مهدداً بنشر تلك الصور إن لم يزودنه بمزيد من الصور والأشرطة الجنسية لهن. يُطلق على أمثال ميهانغوس اسم «راتر» (ratter)، اشتقاقاً من «رات» (RAT) وهي الحروف الأولى لعبارة (Remote Access Trojan) التي تعني «التسلل عن بعد بواسطة [فيروس إلكتروني من نوع] تروجان» [= «فيروس حصان طروادة»]. ويستخدم أولئك الأشخاص فيروسات «تروجان» للتحكم بحاسوبك، بل إن بعض الـ «راتر» الأكثر خفاءً يسيطر بتّودة على كاميرا حاسوبك فيشغلها عن بُعد من دون إشعال ضوء الاستعمال⁽⁷¹⁾. هناك مجموعات من الـ «راتر» لا تبتزّ ضحاياها، لكنها تتاجر بصور الناس وأشرطتها وملفاتهما.

لا يقتصر أمر التسلل عن بُعد على الـ «هاكرز». ففي الفصل 7، تحدّثت عن تلك المدرسة التي تجسّست على تلامذتها بواسطة حواسيبهم. في العام 2012، نجحت «اللجنة الفيدرالية للتجارة» بمقاضاة 7 شركات تبيع الحواسيب بالتقسيت، لكنها كانت تتجسّس على زبائنهم مستخدمةً كاميرات الـ «ويب» في حواسيبهم⁽⁷²⁾.

أثناء تأليف هذا الكتاب، تناهت إلى مسامعي قصة ماثلة رواها شخصان مختلفان. وحكى كل منهما أن صديقاً - بالأحرى ابنته - سجلت في كلية جامعية. وبعد سنوات قليلة، تلقت الابنة رسالة من كلية لم تتقدّم إليها أبداً. ونقلت الرسالة

أن الكلية جمعت معلومات عن الابنة خزنتها لسنوات عدّة، وأن بعض الـ «هاكرز» دخلوا إلى قاعدة بيانات الكلية أخيراً، وسرقوا تلك المعلومات كلها. وكذلك حملت الرسالة الابنة أن تضع تنبيهاً بحصول احتيال على حسابها مع مكاتب إقراض كبرى.

في الحالتين كليهما، حصلت الكلية على معلومات عن الابنة من سمسار، عندما كانت تلك الصبية في نهاية المرحلة الثانوية، سعيًا لاجتذابها إلى صفوف الكلية. وفي الحالتين، لم تكن الصبية قد حاولت أبداً الانتساب إلى الكلية التي بعثت إليها بتلك الرسالة. ولم يحل ذلك دون تخزين الكليتين البيانات لسنوات طويلة، وكذلك لم تقدر أيٌّ منهما على حماية تلك البيانات.

9

التنافسية التجارية

في 1993، كانت الإنترنت مغايرة تماماً لحالها حاضراً. لم تكن التجارة الإلكترونية قد ظهرت، وكانت «الشبكة العنكبوتية العالمية» (*) (World Wide Web) تجتاز طفولتها المبكرة. كانت شبكة الإنترنت أداة اتصال متقدمة لا يستخدمها سوى الأكاديميين ومحترفي التقنية الإلكترونية، كما كنا نستعمل البريد الإلكتروني، ومجموعات الأخبار، إضافة إلى بروتوكول لتبادل المحادثات يشار إليه تقنياً باسم «آي آر سي» (IRC). كانت الحواسيب بدائية، وكذلك حال أمن الكمبيوتر. وطيلة 20 عاماً، نجحت «وكالة الأمن القومي» في الإبقاء على برامج التشفير بمنأى عن التداول الواسع؛ بتصنيفها ذخائر وبالتالي تقييد تصديرها. ولم يتسن للشركات الأميركية التي تنتج برامج أو معدات ذات تشفير قوي أن تباع منتجاتها في الخارج. وتقصّدت الشركات الأميركية وضع تشفير ضعيف - أعني بذلك أنه قابل للاختراق بسهولة - في منتجاتها المحلية والدولية؛ لأن ذلك أكثر سهولة من الحفاظ على نسختين [إحداهما للدخول بتشفير قوي والأخرى للخارج بتشفير ضعيف] من المنتج عينه.

(*) على الرغم من شيوع استخدام مصطلحي "شبكة الإنترنت" و"الشبكة العنكبوتية الدولية" بوصفها شيئاً واحداً، فإن ذلك ليس دقيقاً تماماً. إذ نشأت "العنكبوتية" بمبادرة تقنية من خبير المعلوماتية السري تيم بارنزلي، الذي ابتكر تقنية ربط النصوص، وتلاها الصور وملفات الصوت وأشرطة الفيديو والمواد كافة، فيما تشمل الإنترنت كل ما يحتويه الفضاء السبراني في الكوابل الضوئية لتلك الشبكة، وضمنه "العنكبوتية".

وكان العالم يبدّل أحواله. لم يكن ممكناً إخماد اكتشافات التشفير، كما أن العالم الأكاديمي شرع في الإمساك بقدرات تُشابه ما تملكه «وكالة الأمن القومي». في العام 1993، أُلِفْتُ كتابي الأول التشفيرَ التطبيقي (Applied Cryptography) الذي وضع اكتشافات التشفير في متناول جمهور عام وواسع⁽¹⁾. كان أمراً كبيراً⁽²⁾. وبعثُ 180 ألف نسخة من الكتاب في طبعتين. ووصفته مجلة وايرد العلمية بأنه «الكتاب الذي تَمَتَّ «وكالة الأمن القومي» لو أنه لم يكتب»؛ لأنه يعلم مهارات التشفير لغير المحترفين. جرت البحوث على مستوى عالمي، وشرعت الشركات الناشئة غير الأميركية في وضع تشفير قوي في منتجاتها. ووجدت دراسة جرت في العام 1993، أن ما يزيد على 250 من منتجات التشفير كانت تُصنع وتسوّق خارج الولايات المتحدة⁽³⁾. وخشيت الشركات الأميركية من عدم قدرتها على المنافسة في ذلك المجال؛ نظراً للقيود المفروضة على تصدير منتجات بتشفير قوي.

في الوقت عينه، بدأ القلق يتساب الـ «إف بي آي» بشأن قدرة التشفير القوي على إضعاف قدرتها في التنصّت على محادثات المجرمين. وظهر قلق مماثل بشأن الـ «إيميل»، لكنه أقل من ذلك المتصل بصناديق تشفير الصوت التي يمكن وضعها بسهولة فوق سماعات الهاتف. كانت تلك المرة الأولى التي استخدم فيها الـ «إف بي آي» عبارة «الدخول في الظلام» لوصف مستقبلها المتخيل في ظل التشفير فائق القوة. كانت قصة مرعبة لا تجد ما يبرّرها، تماماً كحالتها حاضراً، لكن المشرّعين صدّقوها⁽⁴⁾. وسرعان ما صاغوا «قانون مساعدة الاتصالات في إنفاذ القانون»، واختصاراً «كاليا»⁽⁵⁾، الذي تحدّث عنه في الفصل 6؛ ومارس الـ «إف بي آي» ضغوطاً عليهم كي يمرّروا قانوناً يحول دون تصدير منتجات بتشفير قوي، من دون وجود «باب خلفي» فيه، يسمح لـ «إف بي آي» بالدخول منه.

بدلاً من ذلك، توصّلت إدارة الرئيس بيل كلينتون إلى حلٍّ: إنّه الـ «كليب شيب» (Clipper Chip). ومثّل الـ «كليب شيب» نظاماً تقنياً للتشفير، أدمجت في دواخله قدرات الرقابة التي طلبتها الـ «إف بي آي» و«وكالة الأمن القومي».

وزُعم أن خوارزميات التشفير كانت قويّة بما يكفي لمنع التنصّت، مع وجود «باب خلفي» يسمح لمن يملك مفتاحه الدخول إلى النص كاملاً. وروّج بوصفه «مفتاح المتعهد»⁽⁶⁾، كما عُدّ تسوية كبيرة تتيح للشركات الأميركية المنافسة عالمياً بتشفيرها القوي، مع الحفاظ على قدرات الـ «إف بي آي» و«وكالة الأمن القومي» في التنصّت.

كانت الأداة الأولى التي احتوت «كليب شيب»⁽⁷⁾ هي الهاتف الآمن الذي صنّعه شركة «إيه تي أند تي» (AT&T) الشهيرة في الاتصالات. لم يكن ذلك هاتفاً خلوياً؛ لأننا كنا لا نزال في 1993. كانت تلك الأداة هي صندوق يوضع بين سماعة الهاتف الخط الأرضي التليفوني، ويعمل على تشفير الصوت. بمعايير تلك الأيام، كان هاتفاً متقدماً، مع صوت بنوعية مقبولة، لكنه عملي.

ولم يشتره أحد.

برؤية استرجاعية، كان شيئاً مكشوفاً. لم يرغب أحد بتشفير مُدمج فيه «باب خلفي» مفتوح على أذني حكومة الولايات المتحدة⁽⁸⁾. لم يرغب فيه الأشخاص المعروفون باهتمامهم بأمور الخصوصية. لم تُردّه الشركات الأميركية. ولم يقبله الناس خارج الولايات المتحدة، خصوصاً مع وجود بدائل غير أميركية تتمتع بتشفير قوي ومن دون «باب خلفي». كانت الحكومة الأميركية هي المشتري الوحيد لتلك الأجهزة التي لم تستعمل أبداً⁽⁹⁾.

خلال السنوات القليلة التالية، جرّبت الحكومة الأميركية مجموعة المبادرات المتصلة بوجود «مفتاح المتعهد»⁽¹⁰⁾، وتضمّنت كلها وجود «أبواب خلفية» تعطي الحكومة الأميركية القدرة على النفاذ إلى التشفير بأكمله، لكن السوق رفض تلك المبادرات كلها، بتعقّل.

بشّرت هزيمة «كليب شيب» ومجمل تجربة التشفير مع «مفتاح المتعهد» بنهاية القيود الحكومية على التشفير القوي. وتدرّجياً، رُفِعَت تلك القيود عن برامج الكمبيوتر في 1996، ثم رُفِعَت عن معظم مكوّنات الأجهزة الإلكترونية في

السنوات القليلة التالية. ولم يكن توقيت ذلك التغير متسرّعا. ففي 1999، كانت السوق العالمية مملوءة بقرابة 800 جهاز فيها تشفير قوي صدرتها 35 دولة، لم تكن الولايات المتحدة من بينها⁽¹¹⁾.

لم يُقَضَّ على «كليب شيب» والقيود على التشفير القوي بأثر من المطالبة باحترام خصوصية المستهلك. بالأحرى، قضت عليهما المنافسة من الدول الأخرى ومتطلبات الشركات الصناعية الأميركية. لقد تطلّب نمو التجارة الإلكترونية وجود التشفير القوي، ولم تستطع «وكالة الأمن القومي» ومكتب الـ «إف بي آي» وقف تطوّره وانتشاره.

رقابة الحكومة تضرب بالتجارة الأميركية

اعتقد كثيرون ممن خاضوا «حروب التشفير»، وفق تسمية كانت رائجة أنهم انتصروا في تسعينيات القرن العشرين⁽¹²⁾. في المقابل، أظهرت وثائق سنودن أن مفهوم زرع «باب خلفي» تنفذ الحكومة الأميركية منه إلى الشيفرة بأكملها، استمر العمل به بصورة سرّية من قبل «وكالة الأمن القومي» والـ «إف بي آي». ولأن سنودن أذاع الأمر على الملأ، شرعت الشركات الأميركية في خسارة زبائنهم في الخارج؛ لأن الآخرين لا يرغبون في رؤية معلوماتهم وبياناتهم متجمعة في يد الحكومة الأميركية.

وتلحق الرقابة التي تمارسها «وكالة الأمن القومي» خسائر بالتجارة الأميركية بواسطة ثلاث طرق مختلفة⁽¹³⁾. إذ بات الناس ينفرون من «سُحْب المعلومات» الأميركية، وهناك انخفاض في مبيعات الحواسيب ومعدّات التشبيك الأميركية، وأخيراً لم يعد أحد يثق بالشركات الأميركية.

في 2013، تكلّفت حقيقة أن «وكالة الأمن القومي» تحصل بواسطة برنامج «بريزم» (PRISM)، على بيانات الجمهور من الشركات الأميركية لخدمات «حوسبة

السحاب»؛ وارتد الأمر بشدة على العلاقات العامة للشركات الأميركية⁽¹⁴⁾. وبصورة شبه فورية، ظهرت مقالات تتحدث عن خسائر في السوق تسجلها الشركات الأميركية العاملة في «حوسبة السحاب» وشريكاتها، لمصلحة الشركات الآتية من بلدان ينظر إليها بوصفها محايدة، كسويسرا⁽¹⁵⁾. في العام 2014، أظهر مسح استطلاعي عن الشركات الكندية والبريطانية أن 25 ٪ منها شرعت في نقل مخازن معلوماتها خارج الولايات المتحدة، حتى لو أدى ذلك إلى انخفاض مستوياتها التقني⁽¹⁶⁾. وبين مسح آخر أن الكشوفات عن «وكالة الأمن القومي» أقلق المدراء التنفيذيين بشأن بياناتهم وتخزينها⁽¹⁷⁾.

تفاوتت التقديرات بشأن خسائر الشركات الأميركية التي تقدم خدمات «حوسبة السحاب»⁽¹⁸⁾. وتوقعت دراسة أجرتها «مؤسسة الابتكار وتقنية المعلومات» (Information Technology & Innovation Foundation) في العام 2013، خسارة في العائدات تتراوح بين 22 و35 بليون دولار في السنوات الثلاث التالية؛ ما يمثل نسبة تتراوح بين 10 ٪ و20 ٪ مما تحصل عليه شركات «حوسبة السحاب» الأميركية من أعمالها خارج بلادها. وتعتقد شركة «فورستر ريسيرش» (Forrester Research) للتحليلات بأن تلك الأرقام منخفضة، إذ تقدر الخسائر بقرابة 180 بليون دولار؛ لأن بعض الشركات الأميركية ستنتقل إلى مقدمي «حوسبة السحاب» في الخارج⁽¹⁹⁾.

وفي ذلك المجال عينه، عانت شركات الكمبيوتر والإنترنت الأميركية ضربات موجعة أيضاً. وفي 2013، أعلنت شركة «سيسكو سيستمز» المختصة في الشبكات الرقمية أنها سجلت رابع خسارة فصلية متتالية وتراوحت بين 8 ٪ و10 ٪⁽²⁰⁾. كذلك سجلت شركة «إيه تي أند تي» للاتصالات خسائر في عائداتها، معلنة أنها تواجه مشكلات في خطط توسعها في السوق الأوروبي⁽²¹⁾. وهناك خسائر لشركة «آي بي أم» في الصين⁽²²⁾، وهو ما ينطبق على حال شركة «كوالكوم» (Qualcomm) الأميركية العاملة في صناعة الحواسيب المتنوعة⁽²³⁾. وخسرت شركة «فيريزون»

الأميركية المختصة في التجارة الإلكترونية عقداً ضخماً مع الحكومة الألمانية⁽²⁴⁾. هناك مزيد من ذلك السيل⁽²⁵⁾. حضرت بنفسي اجتماعات خاصة شكت فيها شركات برامج الكمبيوتر الأميركية من خسائر ضخمة في مبيعاتها الخارجية. وكتب جون شامبرز، المدير التنفيذي لـ «سيسكويستيمز» إلى إدارة الرئيس باراك أوباما، شاكياً من أن اختراق «وكالة الأمن القومي» للمعدات الإلكترونية الأميركية «من شأنه نسف الثقة بصناعتنا وقدرة شركات التكنولوجيا الأميركية على تقديم منتجات تصلح للسوق العالمية»⁽²⁶⁾.

وتردّد شكوى شامبرز أصداء الطريقة الثالثة للضرر الذي حاق بالشركات الأميركية جراء كشوفات سنودن عن رقابة «وكالة الأمن القومي»؛ وهي فقدان الثقة. إذ بات العالم يعرف أن الشركات الأميركية تعطي «وكالة الأمن القومي» منفذاً إلى الهياكل الرئيسة للإنترنت، والشركات العاملة في «حوسبة السحاب» تعطي الوكالة منفذاً لحسابات مستخدميها. وبات العالم يعرف أيضاً أن «وكالة الأمن القومي» تقتحم معدّات الكمبيوترات الأميركية عند تصديرها، وتدسّ فيها خلصة مكوّنات تخدم الرقابة التي تمارسها الوكالة⁽²⁷⁾. وصار العالم على دراية بأن محكمة سرية ترغم الشركات الأميركية على التجاوب مع متطلّبات رقابة «وكالة الأمن القومي»، ثم تأمرها بأن تكذب على الجمهور في ذلك الشأن. هل لنا أن نستعيد قصة «لافايت» في الفصل 5 في هذا الكتاب؟

تفاقت معضلة انعدام الثقة مع التطمينات المتوالية من إدارة الرئيس أوباما بأن «وكالة الأمن القومي» ركّزت معظم جهودها على غير الأميركيين. إذ يأتي ما يزيد على نصف عائدات شركات «حوسبة السحاب» الأميركية من الأسواق الخارجية. وعبر عن ذلك المازق مؤسّس «فيسبوك» مارك زوكربيرغ، أثناء مقابلة في العام 2013، بأفضل الكلمات قائلاً: «تمثّل ردّ الحكومة الأميركية بالقول «لا تقلقوا، لم نكن نتجسّس على الأميركيين». يا للروعة. كم تساعد تلك الكلمات الشركات

التي تسعى إلى التعامل مع الناس في أصقاع العالم قاطبة، وكم توحى بالثقة بشركات الإنترنت الأميركية⁽²⁸⁾.

وإنصافاً، يجدر القول إن ذلك المأزق ربما كان مجرد مشهد عابر نجم من كثافة التغطية الإعلامية للرقابة التي مارستها «وكالة الأمن القومي»، ولا نعلم إلى متى سيستمر. نعلم أنّ بلداناً كثيرة - وألمانيا بلد كبير أيضاً - باتت تحاول صنع «سحابة معلومات» محلية؛ بهدف الحفاظ على بياناتها الوطنية بعيداً عن أيدي الوكالة⁽²⁹⁾. وأخيراً، أصدرت المحاكم الألمانية أحكاماً ضد ممارسات «غوغل»⁽³⁰⁾ و«فيسبوك»⁽³¹⁾ و«آبل»⁽³²⁾ في جمع البيانات؛ كذلك ناقشت الحكومة الألمانية حظر كل الشركات الأميركية التي تتعامل مع «وكالة الأمن القومي»⁽³³⁾. وتتجه خصوصية البيانات لرسم شكل السلامة العامة الجديدة في التجارة الدولية⁽³⁴⁾.

وكذلك تشكّل الخصوصية شرطاً تعاقدياً جديداً. وبأطراد، صارت الشركات الأميركية الكبرى تشترط على مقدمي خدمات تقنية المعلومات لها أن يوقعوا عقوداً تضمن عدم وجود «أبواب خلفية» في النظم المعلوماتية التي يبيعونها للشركات. وبتحديد دقيق، تعمل اللغة التعاقدية على إلزام أولئك الباعة بالآل تتضمن نظمهم شيئاً يسمح لطرف ثالث بالوصول إلى معلومات الشركات وبياناتها. وبذا، يصبح من الصعب على الشركات البائعة للنظم المعلوماتية التعاون مستقبلاً مع «وكالة الأمن القومي» أو وكالات حكومية أخرى؛ لأن ذلك يعرضها إلى مسؤولية قانونية بموجب العقود الموقعة مع زبائنهم من الشركات الكبرى. وفي حال لم يوقعوا تلك العقود وشروطها، فلسوف يخسرونها لمصلحة شركات تقبل التوقيع على تلك الشروط.

ومن الصعب علينا أيضاً معرفة مدى ارتفاع حدة المنافسة مع منتجات وخدمات تُصنّع في دول أخرى⁽³⁵⁾. إذ تتقدم شركات عدّة في أوروبا وآسيا وأميركا الجنوبية، للاستفادة من أجواء الحذر المستجدة⁽³⁶⁾. واستناداً إلى التجربة

مع «حروب الخصوصية» في تسعينيات القرن العشرين، هناك احتمال أن تقدّم مئات من الشركات غير الأميركية منتجات في المعلوماتية لا تطالها القوانين الأميركية⁽³⁷⁾. ويشمل ذلك البرمجيات الرقمية، خدمات «حوسبة السحاب»، مواقع شبكات التواصل الاجتماعي، معدّات الشبكات الإلكترونية، و... كل شيء آخر. وبغض النظر عن مدى مأمونية تلك المنتجات - لأن هناك بلداناً أخرى ربما وضعت «أبواباً خلفية» لها في المعدّات التي تستطيع السيطرة عليها - أو حتى مدى كونها فعلياً خارج قدرة «وكالة الأمن القومي» في النفاذ إليها؛ فلا ريب أن رقابة الوكالة ألحقت ضرراً هائلاً بالتجارة والأعمال الأميركية.

تكلفة رقابة الشركات على التجارة

في زمن سابق، ساد ما يشبه التسليم بمقولة أن لا أحد يدفع ثمن الخصوصية. ولفترة ما، كانت المقولة صحيحة لكن السلوكيات أخذت تتغيّر.

إذ بات الناس أكثر دراية بمن يستطيع النفاذ إلى بياناتهم ومعلوماتهم، وبرزت مؤشّرات عن استعداد بعض الناس في السنوات الأخيرة لأن يدفع مقابل الحفاظ على الخصوصية. في العام 2000، أظهرت دراسة⁽³⁸⁾ أنّ الإنفاق بواسطة الإنترنت سوف يزيد بقرابة 6 بلايين دولار سنوياً، إذا أحس الناس أنهم محميون جيداً أثناء عمليات الشراء⁽³⁹⁾. وفي 2007، خلصت دراسة إلى القول إنّ جمهور المستهلكين لديه استعداد أن يدفع 60 سنتاً لكل سلعة ثمنها 15 دولاراً، مقابل الحصول على حماية لخصوصيته أثناء عمليات الشراء على الإنترنت. وبعد ما كشفته وثائق سنودن، تنشر شركات كثيرة إعلانات عن الحماية من الرقابة الحكومية.

ولا تقدّم معظم الشركات الخصوصية كملح تفضيلي لها في السوق، لكن هناك بعض الاستثناءات⁽⁴⁰⁾. إذ يميّز محرك البحث «داك داك غو» (DuckDuck Go) بأن نمودجه في العمل يستند إلى عدم تتبّع مستخدميه⁽⁴¹⁾. وتقدّم شركة «ويكر» (Wickr) برنامجاً رقمياً لتشفير التراسل الفوري يشمل الصورة وأشرطة الفيديو

والرسائل النصية للخلوي والبريد الإلكتروني، ومحادثات الإنترنت، والملفات المرفقة بالرسائل وغيرها. ويقدم موقع «إيلو» (Ello) منصة للتواصل الاجتماعي لا تتبع مستخدميها⁽⁴²⁾. لا تتمتع تلك الشركات بالقوة والصيت الذي تملكه الشركات الراسخة في تلك الحقول، لكنها تتقدم في أعمالها باطراد.

إذاً، نحن نشهد صعوداً لأهمية الحفاظ على خصوصية المستهلك والزبون، بالتزايد المطرد في عدد الشركات التي استحدثت منصب «مدير الخصوصية». ويُعرف الأخير بأنه مدير تنفيذي يتولى المسؤولية عن المخاطر في السمعة والقانون المتصلة بالمعلومات والبيانات التي تحوزها الشركة. وبات لمديري الخصوصية منظمة خاصة بهم تسمى «رابطة محترفي الخصوصية» (Association of Privacy Professionals)، وشرعوا في إرساء قوانين وقواعد تنظيمية، حتى مع غياب الدعم الحكومي لهم. وينهضون بتلك الأمور لأنها تشكل تجارة مجزية.

10

الخصوصية

لعل المفهوم المغلوط الأكثر شيوعاً عن الخصوصية أنها تتعلق بإخفاء أمر ما⁽¹⁾. ثمة عبارة شائعة تقول: «إن لم ترتكب خطأ، فليس لديك ما تخفيه»، موحية بأن الخصوصية لا تنقذ سوى من يرتكبون أفعالاً مغلوطة.

وبقليل من التفكير، يتبين أنها عبارة لا معنى لها⁽²⁾. ليس خطأ ممارسة الجنس، أو الاغتسال في الحمام أو الغناء تحت «الدوش». ليس خطأ أن نبحت عن وظيفة من دون أن نعلم رب عملنا الراهن. ليس خطأ البحث عن أمكنة تؤمن خصوصيتنا أثناء التأمل أو التحدث عن أمور عاطفية أو شخصية؛ وكذلك الحال عندما نضع رسائلنا في مغلفات خاصة، ونمنح ثقتنا لصديق بعينه دون سواه.

أبعد من ذلك، حتى قائل تلك العبارة لا يؤمنون بها فعلياً. في مقابلة جرت سنة 2009، صاغ المدير التنفيذي لـ «غوغل» إريك شميدت الأمر على النحو التالي: «إذا كان لديك ما لا تريد أي شخص آخر أن يعرفه، فلربما يجب عليك في المقام الأول ألا تفعل ذلك»⁽³⁾. ولكن، في العام 2005، منع شميدت موظفي «غوغل» من التحدث إلى مراسلي موقع «سي نت» الإعلامي؛ لأن أحد المراسلين كشف تفاصيل شخصية عن شميدت في أحد المقالات⁽⁴⁾. وفي العام 2010، صرح مؤسس «فيسبوك» مارك زوكربيرغ بأن الخصوصية لم تعد «عُرفاً اجتماعياً»⁽⁵⁾، لكنه اشترى أربعة منازل قريبة من مسكنه في «بالو ألتو» كي يؤمن خصوصيته⁽⁶⁾.

هناك القليل من الأسرار التي لا نخبر عنها أحداً، ونبقى على ثقة بأن شيئاً من السرية يحوط بها حتى بعد أن نخبر عنها أحداً ما بعينه⁽⁷⁾. وكذلك ندبج رسائل هيمية للأصدقاء والمحبين، ونبوح للطبيب بأشياء لا نخبرها سواه، ونقول أشياء في اجتماعات العمل لا نعلنها على الملأ. ونأخذ أسماء مستعارة للتمييز بين شخصيتنا في العمل وشخصيتنا الفعلية، وكذلك الحال عندما نريد تجربة شيء جديد بطريقة مأمونة⁽⁸⁾.

أظهر مارك زوكربيرغ، المدير التنفيذي لـ «فيسبوك»، سطحية لافتة حين قال: «تملك هوية وحيدة. الأرجح أن الزمن الذي كنت تقدم فيه صورة عنك للأصدقاء والزملاء في العمل تختلف عن تلك التي تقدمها لبقية الناس، أصبح موشكاً على الانتهاء. فمجرد امتلاكك هويتين يعطي نموذجاً عن عدم المصداقية»⁽⁹⁾.

لسنا الشخص نفسه بالنسبة لكل شخص نعرفه أو نصادفه. ونتصرف بطريقة مختلفة مع أصدقائنا وعائلتنا وزملائنا في العمل وما إلى ذلك. نأكل في المطعم بطريقة تختلف عن المنزل. نروي قصصاً لأطفالنا تختلف عما نحكيه لمن نلتقيه في جلسات الشرب. ليس بالضرورة أننا نكذب، على الرغم من أننا نفعل ذلك أحياناً؛ لكننا لا نكشف عن المناحي نفسها من ذاتنا للناس كافة. ذلك شيء إنساني أصيل. يتيح لنا الخصوصية أن نتصرف بطرق تناسب مع الظروف المختلفة التي قد نواجهها. في ظل خصوصية المنزل وغرفة النوم، نسترخي بطريقة تختلف كلياً عما نكونه بوجود آخرين.

إن الخصوصية حق إنساني أصيل، وهو شرط لاستمرارية الشرط الإنساني بكرامة واحترام⁽¹⁰⁾. إنه حق يتصل بمسألة الاختيار وامتلاك ما يكفي من القوة للتحكم بالطريقة التي تقدم بها نفسك إلى العالم. وتفضل دانا بويد المختصة في الثقافات الإثنية على الإنترنت، صوغ المسألة على النحو التالي: «لا تتعلق الخصوصية

بوجود ما يقوم بوكالة ما عنك، بل إن القدرة على تحقيق الخصوصية هي تعبير عن وجود الوكالة»⁽¹¹⁾.

عندما نفقد الخصوصية، نفقد قدرتنا على التحكم بطريقة تقديم أنفسنا⁽¹²⁾. نفقد تلك القدرة عندما تتشارك بالصدفة مجموعة ما على «فيسبوك» أقوالاً لنا، مع مجموعة أخرى، وكذلك نفقد تلك القدرة كلياً عندما تجمع الحكومة بياناتنا ومعلوماتنا. وحينها، نسأل أنفسنا «كيف عرفت الحكومة بالأمر؟ كيف تأتي أنني فقدت التحكم في من يجدر به أن يعرف عن طفولتي المعبّبة، أو بالسخرية الهاذرة، أو قضائي العطلة في جمهورية الدومينيكان؟ ربما تعرف ذلك الشعور جيداً⁽¹³⁾». ربما أحسست به عندما انضمت أمك إلى قائمة أصدقائك على «فيسبوك» أو أي شبكة اجتماعية تعدّها حيزاً لك ولأصدقائك. الاعتداءات على الخصوصية هي انتهاكات تقتحم حياتنا⁽¹⁴⁾.

ثمة أساس فيزيولوجي للخصوصية⁽¹⁵⁾. إذ يشدّد بيتر واتس، وهو اختصاصي في البيولوجيا، على أن الرغبة في الخصوصية أمر أصيل وليس مكتسباً؛ مشيراً إلى أن الحيوانات اللبونة تضحي أقل تجاوباً في ظل وجود رقابة. نعتبر الرقابة تهديداً مادياً وجسدياً؛ لأن الحيوانات في عوالم الطبيعة تُراقب من قبل من يسعى إلى افتراسها. تجعلنا الرقابة نحس كأننا فرائس، تماماً مثلما تجعل من يراقبنا يتصرّفون كمفترسين⁽¹⁶⁾.

كتب الفلاسفة والروائيون وعلماء النفس والاجتماع والمختصون بالتقنيات عن تأثير الرقابة الدائمة، بل حتى مجرد وجود انطباع بالرقابة الدائمة. وبيّنت الدراسات أيضاً أننا نكون حينها أقل تمتعاً بالصحة جسدياً ونفسياً⁽¹⁷⁾. وتتملكنا مشاعر الكآبة والتوتر وتضاؤل القيمة الذاتية. تجرّدنا الرقابة من كرامتنا⁽¹⁸⁾. وتهدّد ذاوتنا كأفراد⁽¹⁹⁾. في سجون العالم ومعقلاته كافة، تستعمل الرقابة الدائمة أداة تكتيكية لسلخ الفرد عن إنسانيته.

ليست الاعتداءات على الخصوصية بمتساوية؛ ذلك أن السياق التي تحصل فيها يصنع الفارق بين بعضها بعضاً. هناك فارق بين أن يعثر ضابط في «أمن إدارة النقل» على مواد إباحية في حقيبتك، وبين أن تعثر عليها زوجته. ثمة فارق بين معرفة الشرطة بأمر تعاطيك بعض المواد، وبين معرفة أصدقائك بذلك الأمر. وكذلك لا تتساوى الأضرار الناجمة عن الاعتداءات على الخصوصية. إذ تكون أشد تأثيراً في من يعيش في الهوامش الاجتماعية - الاقتصادية، ومن ينتمون إلى مجموعات مهمشة عرقياً وسياسياً وإثنيًا ودينيًا. وكذلك حال من يشغلون مناصب مهمة ويكونون عرضة لاستمرار موافقة الناس على ما يفعلون. إن حياة بعضنا تعتمد كلياً على الخصوصية.

وباتت خصوصيتنا عرضة للغزو من الرقابة الدائمة. وأصبح ضرورياً فهم كيفية حدوث ذلك الغزو كشرط لفهم الرهانات المتصلة به.

الزائل

على مر التاريخ، اتسمت محادثتنا وتفاعلاتنا مع بعضنا بعضاً بطابع الزوال. إنها الطريقة التي نفكر بها عادة بالمحادثة. كانت الاستثناءات عن تلك القاعدة نادرة إلى حد أنها تستحق التسجيل: مفكرة محفوظة، كاتب يدون بطريقة الاختزال وثنائى عن مجريات المحكمة، مرشح سياسي يصنع خطاباً مسجلاً.

تغير ذلك تماماً. صارت الشركات تجري عدداً أقل من المقابلات الشخصية المباشرة. ويتواصل الأصدقاء مع بعضهم بعضاً بواسطة الإنترنت. خضت زوجتي محادثات حميمة برسائل الخلوي النصية. نتصرف جميعنا كأن تلك المحادثات زائلة، لكنها لم تعد كذلك. إذ باتت تخزن بطرق لا نملك أي سيطرة عليها.

يصعب التخلص من المحادثات المدونة. تلقى الجنرال أوليفر نورث ذلك الدرس مبكراً في العام 1987⁽²⁰⁾. إذ تبين له أن الرسائل التي ظن أنه حذفها منها،

كانت محفوظة في نظام إلكتروني خاص بالموظفين الكبار في البيت الأبيض، ما يمكن اعتباره شكلاً أولياً من البريد الإلكتروني. وبعد عشر سنوات، تعلم بيل غيتس الدرس نفسه، عندما قُدِّمت محادثاته بواسطة البريد الإلكتروني إلى القضاء كجزء من التحقيق في الدعوى التي رُفِّعت بشأن احتكارية «مايكروسوفت»⁽²¹⁾. وتلقَّى 100 نجم ونجمة الدرس نفسه في العام 2014، عندما سُرقَت صور شخصية حميمة لهم - بعضها كان يعدُّ مخدوفاً - من سحابة رقمية لشركة «آبل» تحمل اسم «آي كلاود» (iCloud)، وجرى تشاركها على نطاق أوسع كثيراً مما قصد أصحابها بشأنها⁽²²⁾.

صار الزوال شأنًا فائق الصعوبة. لا يزال معظم المحادثات الشفوية خارج التسجيل، لكن إلى متى سيستمر ذلك؟ في متاجر البيع بالتجزئة، يسجل نظام رقمي للمراقبة وجودنا، حتى لو لم نفعل سوى تقليب المعروضات، وحتى لو دفعنا كل مشترياتنا نقداً. تسجل بعض البارات أرقام البطاقة الشخصية لكل من يدخلها⁽²³⁾. وعلى الطائرة، لم يعد مستطاعاً شراء زجاجة نبيذ إلا ببطاقة الائتمان. ولسوف يزداد الأمر سوءاً مع استمرار الميل إلى التسجيل الواسع لمناحي الحياة كافة.

وصف كاتب الخيال العلمي تشارلز ستروس ذلك الأمر بأنه نهاية ما قبل التاريخ⁽²⁴⁾. لن ننسى شيئاً لأننا سنقدر دوماً على استرجاعه من الذاكرة الرقمية لحاسوب ما⁽²⁵⁾. إنه لأمر مستجد على النوع البشري برمته، ولسوف يكون كنزاً لمؤرخي المستقبل، وللأفراد المعاصرين ممن يسعون إلى الحصول على بيانات أفضل من أجل التأمل والتقييم الذاتي.

سوف تغير القدرة على تدوين كل شيء بما يجعله متوافراً إلى الأبد الأفراد والمجتمعات معاً⁽²⁶⁾. ليست ذاكرتنا ولا انطباعاتنا بمثل الثبات الذي نتوقعه. ثمة ما لا نلاحظه، حتى بعض الأشياء المهمة. ونتذكر أشياء كثيرة بطريقة مغلوطة، حتى إننا لا نكون متأكدين من استعادته بصواب⁽²⁷⁾. كذلك ننسى أشياء مهمة كنا

نعتقد أننا لن ننساها أبداً. من يدأب على الكتابة في مفكرته يعرف تلك الظاهرة جيداً، وهي أن ما كتبناه قديماً يبدو كأنه كتب بأيدي أخرى. أنا أيضاً لاحظتُ أن الاحتفاظ برسائلي الإلكترونية كلها طيلة عشرين سنة، تصنع فارقاً كبيراً في تفكيري عن تاريخي الشخصي.

يملك ربع البالغين الأميركيين سجلات جرمية. حتى المخالفات البسيطة ربما لاحقت الناس طيلة حياتهم مخلّفة آثاراً واسعة عليها⁽²⁸⁾ - لذلك السبب، تلجأ بعض الحكومات إلى محو السجلات الإجرامية بعد مرور زمن معين عليها. ويعني فقدان الزائل أن كل ما تقوله وتفعله يبقى يلاحقك إلى آخر العمر⁽²⁹⁾.

يمثل إجراء محادثات تتلاشى بمجرد حدوثها عرفاً اجتماعياً يتيح لنا راحة واسترخاء كبيرين، وأن نقول أشياء ما كنّا لنقولها بحضور جهاز تسجيل. وعلى مدى أبعد، يشكّل النسيان - والخطأ في التذكّر - ركناً في تعاملنا مع تاريخنا. إذ يمثل النسيان مساعداً قوياً للغفران. إذ تبهت الذاكرة الفردية والجماعية، فيصبح الماضي أقل حدة؛ ما يسمح لنا بغفران الإساءات الماضية. يصعب إقناعي بأن زواجي سيكون أفضل لو جرى الاحتفاظ بسجل تفصيلي عن المشاجرات والنقاشات كلها. يؤدي فقدان الزائل إلى تغيير اجتماعي ونفسي هائل، وهو ليس من النوع الذي لا يبدو أن مجتمعا مستعد له.

الرقابة بالخوارزميات

تتمثل إحدى الحجج الأكثر شيوعاً بشأن الرقابة الجماعية في القول إنها تجري بموجب جداول الرياضيات الحاسوبية، وتسمى تقنياً «خوارزميات» (Algorithms)، وليس وفقاً للأشخاص، ما يعني أنها لا تنتهك خصوصيات الناس. ما ذلك إلا بهتان صريح⁽³⁰⁾.

هناك فارق مهم في السياسة بين رقابتي البشر والحاسوب. ومنذ أن أمدّ سنودن الصحافة بخزّان من الوثائق فائقة السريّة، أضحي الناس على دراية بتلاعب «وكالة الأمن القومي» بالكلمات⁽³¹⁾. إذ تملك كلمة «جمع» تعريفاً محدّداً في وزارة الدفاع الأميركيّة⁽³²⁾. إنها لا تعني جمعاً؛ بل تفيد بأن هناك شخصاً ينظر في تلك البيانات ويحلّل تلك المعلومات⁽³³⁾. في العام 2013، شبّه جايمس كلاير، رئيس «الاستخبارات القوميّة»، خزّان المعلومات في «وكالة الأمن القومي» بالمكتبة. «الكتب كلّها مخزّنة على الرفوف، لكن قلّة منها تُقرأ فعلياً»⁽³⁴⁾. إذاً، تتمثّل مهمّتنا المتصلة بالحفاظ على الأمن والحريات المدنيّة والخصوصيّة، في أن نكون على أقصى درجات الدقّة عندما نذهب إلى تلك المكتبة ونبحث عن الكتب التي نرغب في قراءتها فعلياً.

فكّر في صديق لك يملك آلافاً من الكتب في منزله. وفق كلاير، لا يملك ذلك الصديق سوى الكتب التي قرأها فعلياً!

وللسبب عينه، يصرّ كلاير على أنّه لم يكذب أثناء مثوله للجنة استماع في مجلس الشيوخ⁽³⁵⁾، عندما أجاب بـ «كلا» عن سؤال: «هل تجمع «وكالة الأمن القومي» أي نوع من البيانات عن ملايين أو عشرات ملايين الأميركيّين؟ من وجهة نظر الجيش، لا يشكّل الأمر رقابة إلا إذا نظر شخص ما إلى البيانات وقرأ المعلومات، حتى لو كانت الجداول الخوارزمية التي طوّرتها وزارة الدفاع والشركات المتعاقدة معها، قد حلّلتها المرّة تلو المرّة.

ليست تلك المرّة الأولى التي تُردّد فيها تلك الحجة. إذ إنّها مثّلت ركناً أساسياً في دفاع «غوغل» عن صنعه إعلانات يجري توجيهها بموجب مضامين لها طابع حسّاس وشخصي، في الأيام الأولى لظهور البريد الإلكتروني «جي ميل». إذ تنظر الأجهزة الذكيّة التي تملكها شركة «غوغل» في البريد الشخصي للأفراد، ثم تُدخل إعلانات تناسب مع مضمون كل بريد على حدة، في ذيل الرسائل. ولكن، لا يقرأ

أشخاص رسائل ذلك البريد، بل ينهض الحاسوب وحده بتلك المهمة⁽³⁶⁾. ووفق ما أسرّ به لي شخصياً أحد مسؤولي «غوغل» أثناء الأيام الأولى لإنشاء «جي ميل»، «يشبه القلق بشأن قراءة الكمبيوتر لبريدك أن تحسّ بالقلق لأن كلبك رآك عارياً».

لكن ذلك ليس صحيحاً، بل إن مثل الكلب يدحضه تماماً. عندما يشاهدك كلب عارياً، لا يتأبك القلق بسبب ثلاثة أمور رئيسة: إذ لا يستطيع الكلب أن يفهم ويعي ذلك المشهد، مثلما يفعل أي شخص. ولا يؤسّس الكلب قرارات مستقبلية أو يصنع ذكريات عن ذلك المشهد، ليس بالطريقة التي تحدث عند البشر. ولا يستطيع الكلب أن يخبر شخصاً أو حتى كلباً، عن مشاهدته لك عارياً.

وعندما يراقبك كمبيوتر، تنتفي أسس المقارنة مع الكلب. إذ يستطيع الكمبيوتر أن يتعامل بذكاء مع ما يشاهده، كما يؤسّس قراراته على ذلك. ربما قيل لك إن الكمبيوتر لا يخترن معلومات عنك، لكن لا أحد يقدم لك برهاناً على ذلك⁽³⁷⁾. ولربما قيل لك أيضاً إن الكمبيوتر لن يلفت نظر أي شخص إذا تقاطعت بياناته ومعلوماته عنك بطريقة «مثيرة للاهتمام»، لكن لا أحد يقدم لك تأكيداً عن ذلك. وليس من طريقة للتثبت من أن شخصاً لن يطّلع ويتفهم الخلاصات التي صاغها الكمبيوتر بشأنك، وأن لا أحد سيستخدم بيانات الكمبيوتر في ممارسة تمييز ضدك أو إصدار أحكام بشأنك، بالاستناد إلى مشاهدات الكمبيوتر عنك.

أبعد من ذلك، عندما يخترن الكمبيوتر، يحضر دوماً خطر الانكشاف. من الممكن أن تتغير قوانين الخصوصية في أي وقت، فتتيح استعمال بياناتك القديمة من دون موافقتك الصريحة. كذلك ثمة احتمال أن يحدث اختراق وسطو للبيانات من الـ «هاكرز» أو تنظيمات إجرامية. وتستطيع المنظمة التي تحصل على بياناتك أن تستخدمها بطرق جديدة مع كشفها للعلن، أو تبيعها لمنظمات أخرى. ويستطيع الـ «إف بي آي» أن يرسل مذكرة أمن قومي إلى من يملك بياناتك، فيحصل عليها.

من ناحية أخرى، لا تستطيع أي محكمة على وجه الأرض أن تحصل على وصف لمشهدك عارياً من الكلب الذي شاهدك حينها.

يكنم الفارق الرئيس بين الكلب والكمبيوتر في أن الكلب لا يستطيع التواصل مع أشخاص آخرين بشأن إيصال البيانات والمعلومات عنك، بطريقة تكون مجدية إلى حدٍ يثير قلقك⁽³⁸⁾. إذ يكتب بشرُ الجداول الخوارزمية للكمبيوتر، وكذلك يجري بشرٌ تحليلاً لنتائج تلك الجداول. وعندما نفكر في رقابة خوارزميات الكمبيوتر المفروضة علينا، وما تعطيه من قدرة على تحليل معلوماتنا، يجدر أن نفكر بالأشخاص الذين يقفون خلف تلك الخوارزميات. إذ تصبح تلك الخوارزميات رقابة إذا دقق أشخاص بها، إضافة إلى حقيقتين هما أنهم يستطيعون ذلك، وأنهم يوجهون الخوارزميات بما يجعلها رقابة.

أنت تعرف جيداً أن تلك الأمور صحيحة. إذا اعتقدت أن كلاير محق في كلامه عن الكمبيوتر والكلب، فلن تعترض على وضع كاميرا للرقابة في غرفة نومك، طالما أن هنالك قوانين تتحكم بقدرة الشرطة على التدقيق بها.

كذلك لن تعترض على إجبارك على ارتداء جهاز إلكتروني يثبت إلى جهات حكومية كل ما تقوله على مدار الساعة، طالما أن الموظفين الحكوميين الذين يلتقطون ذلك البث يلتزمون بقوانين تضبط عملهم. في المقابل، إذا كنت تعترض على الأمور السابقة⁽³⁹⁾، فذلك يرجع إلى إدراكك أن خصوصيتك تتأذى من الجمع المؤتمت للمعلومات والبيانات، وعمليات تحليلها بواسطة خوارزميات الكمبيوتر، بغض النظر عن موقع العنصر البشري في تلك العمليات.

تحديد الهوية وإغفالها

مررنا جميعاً بتجربة التعريف عن أنفسنا على الإنترنت. وتربط بعض مواقع الإنترنت هويتك الفعلية مع هويتك الشبكية، كمواقع البنوك والمؤسسات الحكومية

وغيرها. ويربط بعضها هويتك الشبكية مع نظام للدفع - غالباً ببطاقة الائتمان -، وبعضها الآخر يربط تلك الهوية مع حسابك البنكي أو هاتفك الخلوي. ولا تبدي بعض المواقع اهتماماً بهويتك الفعلية، فتتيح لك أن تستخدم اسماً مميزاً فيها. ثمة كثير من المواقع التي تستطيع أن تعمل بتلك الطريقة. ومثلاً، من الممكن تصميم مخزن «آي تيونز» التابع لشركة «آبل» بطريقة لا تتضمن معرفته هويتك فعلياً لمجرد منحك القدرة على الوصول إلى بعض ملفات الموسيقى والفيديو.

تشمل طرق التعريف بالهوية والتثبت من أصالتها، استعمال كلمات المرور، والقياسات البيولوجية التي تعرف باسم «بيومتريكس» (Biometrics) والتذكارات⁽⁴⁰⁾. كنتُ من بين الذين كتبوا بتوسّع عن نُظم التعرّف إلى الهوية والتثبت منها، والمقارنة بينها في القوة ونقاط الضعف. ومن دون الخوض في التفاصيل، تتمثل الخلاصة في أن لا نظاماً كاملاً، لكنها بعمومها جيّدة في أداء ما أعدت من أجله. وبصورة أساسية، تعمل نظم التثبت من الهوية بكفاءة.

وترجع تلك الكفاءة إلى أن مستخدمي تلك النظم يطلبون بأنفسهم أن يجري التثبت من هويتهم. عندما تستخدم بريد «هوت ميل» الإلكتروني، فأنت تريده أن يقتنع بأن ما تستعمله هو حسابك فعلياً، كما تريد إقناع البنك بأن تلك هي نقودك. في المقابل، ربما لا ترغب في أن تربط شركة «إيه تي أند تي» هويتك مع زيارتك لمواقع الإنترنت كافة التي تجربها بهاتفك الذكي؛ لكنك ترغب في أن تحوّل تلك الشركة مكالماتك كافة إلى ذلك الهاتف. تحاول تلك النظم كلها أن تجيب عن سؤال هو: «هل ذلك الفرد هو الشخص الذي يزعمه فعلياً؟» ولذا يكون من السهل جمع البيانات عنا من شبكة الإنترنت، بمعنى أن معظمها يأتي من مصادر حرصنا نحن على تعريفها بأنفسنا.

هناك صعوبة كبيرة في الربط بين تحرّك غُفل الهوية على الإنترنت، وبين شخص محدّد بعينه. إذ ربما لا يكون الشخص راغباً في التعرّف إليه. يكتب تعليقاً مغفل

الهوية على أحد المواقع الشبكية، أو ربما يطلق هجوماً إلكترونيًا في الفضاء السبراني بواسطة شبكتك. في تلك الحال يجب على النظم الرقمية أن تجيب عن سؤال أشد صعوبة هو: «من يكون ذلك المجهول»؟

على المستوى الأساسي تماماً، لا نستطيع التعرف إلى النثر المستقلة من المكونات الإلكترونية أو البرامج الرقمية، عندما يتخذ الخصم المراوغ قراراً بالتهرب من عمليات التعرف إلى هويته. لا نستطيع استخلاص معلومات من حزم متناثرة من البيانات تدور في فضاء الإنترنت. لا نستطيع التثبت من هوية شخص مجهول يجلس خلف لوحة مفاتيح إلكترونية في مكان ما على الكرة الأرضية. وليس من المستطاع التوصل إلى حلّ لتلك المشكلة بواسطة هندسة معينة للنظم الإلكترونية؛ لأنّ ذلك الضعف كامن في صلب طريقة عمل الإنترنت.

ويعني ذلك أننا لا نستطيع الجزم بشأن من ترك تعليقاً مغفل الهوية على مدوّنة إلكترونية. (إذ يحتمل أن يكتب من كومبيوتر عام، أو حاسوب يحتوي عنواناً تعريفياً مشتركاً). لا نستطيع الجزم بشأن هوية من بعث برسالة إلكترونية. من المستطاع تزيف المقدمات التعريفية، وهو أمر يفعله من يطلقون سيول الرسائل المتطفلة التي تشتهر باسم «سبام» (Spam). لا نستطيع الجزم بشأن آلاف المحاولات المتتالية الفاشلة للدخول إلى حسابك البنكي، ولا من يشن هجمات إلكترونية تستهدف البنية التحتية للبلاد.

حتى إننا لا نستطيع الجزم إن كانت تلك الهجمة الإلكترونية تمثل نشاطاً إجرامياً، أو عملاً عسكرياً، أو التعرف إلى الحكومة التي تقف وراءها⁽⁴¹⁾. إنّ الهجمات السبرانية ضد أستراليا في العام 2007، وهي غالباً ما توصف بـ «الحرب السبرانية الأولى»؛ إما شنتها الحكومة الروسية أو شاب في الـ 22 من العمر غلبته أهواؤه⁽⁴²⁾.

عندما ننجح في الربط بين هوية ما وهجمة إلكترونية معينة - كالقول إنها تأتي من مدير ثانوية سيئ الطوية، أو سارق بنك، أو مجموعة تدعمها حكومة ما - فإننا نفعل

ذلك بعد تحقيق جنائي موسّع، أو لأن المهاجم أتاح التعرّف إليه بطريقة أو أخرى. إذ استغرق الأمر شهوراً كي يتعرّف المحللون إلى الصين بوصفها مصدراً محدداً للهجمات الإلكترونية التي استهدفت صحيفة نيويورك تايمس في 2012⁽⁴³⁾؛ كما لم نعرف تحديداً من صنع الفيروس الإلكتروني «ستاكس نت» إلى أن أقرت الولايات المتحدة بذلك⁽⁴⁴⁾. إنها مسألة صعبة تماماً، ومن المرجح ألا نتمكن من إيجاد حل لها في مستقبل قريب.

على مرّ السنين، قدّمت حلولاً عدّة لوضع حد لإغفال الهوية على الإنترنت⁽⁴⁵⁾. وكانت الفكرة وراء ذلك أنه إذا كان ممكناً ربط الهوية بالأعمال كافة على الإنترنت - بمعنى الربط بين العمل ومصدره - يغدو من السهولة بمكان التعرّف إلى المجرمين ومطلقي بريد الـ «سبام»، والمتربصين بالناس، ومتصيدي الثروات على الإنترنت. واختصاراً، يصبح لكل منا على الإنترنت ما يعادل رخصة القيادة.

إنّه هدف مستحيل. أولاً، لا يوجد في العالم الفعلي بنية تحتية لتعطي كل مستخدمي الإنترنت أوراقاً ثبوتية تستند إلى نُظم التعريف الفعلية الأخرى - جواز السفر، وبطاقة الهوية، ورخصة القيادة وأي شيء مماثل - وهو ما نحتاجه للوصول إلى تلك النقطة من التعرّف إلى هويات مستخدمي الإنترنت. وبالتأكيد لا نملك بنية تحتية من ذلك النوع تستطيع أن تشمل العالم بأسره.

حتى لو توصلنا إلى شيء كذلك، فلسوف يستحيل جعله مأموناً. إذا عاش كل منا التجربة المقلقة لرؤية مراهقين يحاولون شراء شراب كحولي قبل بلوغهم سن الرشد، على الرغم من أن ذلك يتعلّق بمقابلة مباشرة تجري وجهاً لوجه. ولن يكون النظام المقترح أعلاه بأفضل حالاً من ذلك. وحتى لو توصل إلى مستوى أفضل، فلن يكون عملياً. ومن المستطاع دوماً وضع نظام لتفعيل الهوية ضمن نظم التعريف بالهوية. ويقلق بلد كالصين من تلك الحقيقة؛ لأنه يريد معرفة الهوية الحقيقية لكل من يستعمل الإنترنت في أراضيه⁽⁴⁶⁾.

لربما بدت تلك الكلمات متناقضة مع ما ورد في الفصل 3 حول سهولة التعرف في الإنترنت إلى الأشخاص الذين يسعون لإخفاء هويتهم. إذ يحصل ذلك بسهولة عندما تتوافر كميات كافية من المعلومات كي تربط بعضها بعضاً، إضافة إلى زمن كافٍ للتدقيق فيها. وتشكل الرقابة الواسعة للجموع الطريقة الوحيدة لتقليص عمليات إغفال الهوية على الإنترنت. وفي الفصل 3، استندت الأمثلة كلها إلى الربط بين نفث كثيرة من المؤثرات، مع الحصول على وقت كافٍ للتحقيق فيها. في المقابل، يغدو صعباً بما لا يقاس التدقيق في كل اتصال إلكتروني على الإنترنت وصولاً إلى مصدره، كأن يجري التدقيق في كل رسالة إلكترونية وحيدة، ووصلة شبكية مفردة وهجمة رقمية بمفردها.

يبقى السؤال مفتوحاً عن مدى القدرة على إيكال عمليات التعرف إلى الهوية بتحليل البيانات وربطها إلى الآلات الذكية. هل من المستطاع صنع نظام حاسوبي متقدم الذكاء بما يتيح له تحليل معلومات الرقابة للتوصل إلى التعرف إلى الهويات الفردية للناس بما يشبه الأمثلة التي عرضها الفصل 3، على نطاق واسع تماماً؟ ربما لا نملك ذلك الآن، ولكن الوقت لن يطول قبل ظهور نظام كذلك.

ثمة جهود تبذل في ذلك الاتجاه. إذ ترغب بلدان كالصين وروسيا في صنع نُظم مؤتمتة للتعرف إلى هوية الأصوات المعارضة على الإنترنت. وتسعى شركات الترفيه للحصول على نُظم مُشابهة للتعرف إلى من يقرصنون الأفلام والموسيقى. وترغب حكومة الولايات المتحدة بتلك النُظم كي تتعرف إلى المنظمات والأشخاص الذين تحسّ بأنهم يمثلون خطراً عليها، بداية من الأفراد المعزولين ووصولاً إلى الحكومات الأجنبية.

في 2012، صرح وزير الدفاع ليون بانيتا علانية بأن «الولايات المتحدة أحرزت تقدماً ملفتاً... في التعرف إلى مصادر الهجمات السبرانية»⁽⁴⁷⁾. ويذهب بي الظن إلى أن أميركا لم تحرز تقدماً جديداً في هندسة الكمبيوتر وعلومه يكفل لها قلب الموازين

جذرياً في التوازن بين عمليات التعرف إلى الهوية وإغفالها على الإنترنت. والأرجح أنها نجحت في اختراق شبكات الخصوم بشكل عميق إلى حد يكفل لها التجسس عليهم والتعرف إلى خططهم.

بديهي القول أيضاً إن تغفيل الهوية سيف ذو حدين؛ لأنه ربما استخدم لحماية خطابات الكراهية والنشاط الإجرامي. ولكن، بينما يصح الحديث عن أهمية عمليات التعرف إلى الهوية، فإن تغفيل الهوية مهم أيضاً للأسباب التي بيّنتها في هذا الفصل. ويعني ذلك أنها تحمي الخصوصية، وتزيد في تمكين الأفراد، إضافة لكونها شرطاً أساسياً للحرية.

11

الامن

يملك الأمن أهمية كبيرة في حياتنا. وتشكل الجريمة والإرهاب والعدوان الخارجي تهديدات تطالنا في الفضاء الافتراضي وخارجيه. بديهي القول إنها ليست التهديدات الوحيدة، لكنني صرفت معظم الفصول السابقة في تبيان تهديدات أخرى. تلزمنا حماية من مجموعة تهديدات متكاملة، ومن هذه النقطة تبدأ المشكلات. لا جدوى من إنكار خطر الأجهزة الشرطية المتغولة أو الحكومة الطاغية، بدعوى حماية أنفسنا من الإرهاب؛ أو إنكار خطر الإرهاب بهدف النجاة من انفلات الأجهزة الشرطية.

وللأسف، عندما يميل المجتمع إلى التركيز على خطر معين، فإنه غالباً ما يهون من شأن بقية المخاطر. والأسوأ من ذلك أننا نميل إلى التركيز على خطر نادر عندما يسدد ضربة مشهدية ضخمة، فيما نتجاهل مخاطر أكثر شيوعاً وتكراراً وعادية⁽¹⁾. ولذا، نخاف من الطيران أكثر من قيادة السيارة، على الرغم من أن الأولى أكثر أماناً. ونخشى الإرهابيين أكثر من الشرطة، على الرغم من أن الأميركي معرض لأن يقتل على يد ضابط شرطة بتسعة أضعاف تعرضه للموت على يد إرهابي⁽²⁾.

بذا، تعترض المخاوف طريق التوصل إلى أمن ذكي. ليس من بُعد النظر الاتكال على استراتيجية تحمي من مخاطر معينة على حساب أخرى، بل يجدر بنا التوصل إلى طرق تضمن التوازن في ضمان الأمن ضد المخاطر كلها.

الأمن في مواجهة الإرهابيين والمجرمين

استخدمت «وكالة الأمن القومي» تكراراً صورة مجازية هي «التوصيل بين النقط»؛ كي تبرّر نشاطاتها الرقابية⁽³⁾. ومرة تلو الأخرى؛ بعد ضربات 9/11، وعقب المفجّر الذي دسّ متفجرات في ملابسه الداخلية، وبعد تفجيرات «ماراثون بوسطن» وغيرها؛ انتقدت الحكومة لأنها لم تعمل على التوصيل بين النقط.

في المقابل، إنّ تلك الصورة المجازية عن توصيل النقط هي مضلّلة تماماً. إذ يسهل التوصيل بين النقط في كتب الرسم الملونة المعدة للأطفال؛ لأنها مرقمة ومرئية بوضوح. أما في الحياة الفعلية، فلا ترى النقاط إلا بعد ظهور حقائق.

لا يمتنعنا ذلك من الإلحاح على معرفة سبب عدم قيام الحكومة بتوصيل النقط⁽⁴⁾. وبرؤية استرجاعية، يمكن القول إنّ هنالك علامات منذرة صدرت بوضوح عن مفجّر مطلق النار في ثكنة «فورت هود»، مفجّر «ماراثون بوسطن»، ومطلق النار في مدرسة «إيسلا فيستا». يسمّي الكاتب نسيم طالب ذلك الأمر بـ «مغالطة السرد»⁽⁵⁾. ومن طبيعة البشر الميل إلى إخبار القصص، وغالباً ما يكون عالم القصة أكثر انتظاماً وتوقعية وانسجاماً من العالم الفعلي. إذ يتصرّف ملايين الناس بطرق فيها من الغرابة ما يكفي للفت أنظار الـ «إف بي آي»، لكن غالبيتهم الساحقة لا يشكلون خطراً. تضم قائمة «أمن إدارة النقل» قرابة عشرين ألف شخص ممنوعين من السفر جواً⁽⁶⁾. وتحتوي القائمة المعروفة باسم «قائمة الموضوعين تحت الرقابة»⁽⁷⁾، قرابة 680 ألف شخص، لكن 40 ٪ منهم «لا يملكون انتهاكات معروفة لتنظيمات إرهابية».

يُقدّم التنقيب في المعلومات بوصفه التقنية الكفيلة بتمكيننا من توصيل النقط. وتنجح الشركات تماماً في التنقيب في بياناتنا الشخصية كي توجّه إعلاناتها بدقة، وترصد التزوير المالي وتنهض بمهام أخرى، فيما تتصب ثلاث قضايا حساسة في وجه تحويل التنقيب في البيانات أداة كفوءة في العثور على الإرهابيين.

تتجسد القضية الأولى والأكثر أهمية في معدلات الأخطاء. ففي الإعلانات، يكون التنقيب في المعلومات أداة ناجعة حتى في ظل نسب مرتفعة من معدلات الأخطاء، لكن العثور على الإرهابيين يتطلب درجة من الدقة أعلى كثيراً، ليس بوسع نُظم التنقيب في البيانات تحقيقها.

إذ يكون التنقيب في المعلومات ناجحاً عندما تبحث عن بروفایل محدّد تماماً، وعندما تكون هناك مناسبات متكررة سنوياً ويكون ثمن الإنذار الخاطيء زهيداً. ويقدم تقصي تزوير بطاقات الائتمان قصة نجاح بارزة لقدرة التنقيب في البيانات في مجال الأمن⁽⁸⁾. وتتقّب شركات البطاقات الائتمانية كلها في قواعد بياناتها للعثور على نمط من الإنفاق يوحي بسرقة بطاقة ائتمان. في الولايات المتحدة، يجري التداول بقرابة بليون بطاقة ائتمان مفعلة، ويطاول التزوير قرابة 8 ٪ منها⁽⁹⁾.

يتشارك كثير من بطاقات الائتمان المسروقة في نمط معين - هو الشراء من أمكنة غير مألوفة بالنسبة لصاحب البطاقة الأصلي، إضافة إلى شراء سلع سياحية مرفقة، وأشياء يسهل حملها - ما يعطي نُظم التنقيب في المعلومات القدرة على تقليص الخسائر بكشفها معاملات مالية مزورة. ولا تزيد كلفة الإنذار الخطأ عن مكالمة تليفونية لصاحب البطاقة تطلب منه تأكيد حصول بعض عمليات الشراء.

وعلى نحو مماثل، تستخدم «وكالة المداخل الداخلية» تقنية التنقيب في البيانات للتعرف إلى المتهمين من الضرائب⁽¹⁰⁾؛ كما تستعملها الشرطة لتحديد النقاط الساخنة المرشحة لحدوث جرائم فيها⁽¹¹⁾؛ كما تستخدمها البنوك لتوقع حالات عدم القدرة على سداد الديون. نالت تلك الأنماط من استخدام تقنية التنقيب في المعلومات حظوظاً متفاوتة من النجاح، وفقاً لنوعية المعلومات والبرامج، لكنها تظل ضمن إطار ما تستطيع تلك التقنية إنجازه.

يختلف الأمر مع مخططات الإرهابيين، غالباً بسبب كثرة المعاملات المزورة مقابل ندرة ضربات الإرهاب⁽¹²⁾. ويعني ذلك أن نُظْم توقع الإرهاب تبقى مكتظة بالإبذارات المغلوطة، مهما كانت دقة النُظْم عالية⁽¹³⁾.

يعود السبب في ذلك إلى رياضيات نُظْم التنقيب في البيانات. هناك أخطاء في نُظْم التقصي كلّها، ويستطيع مصمّمو النُظْم ضبطها بما يكفل تقليل هوامش الإبذارات الكاذبة إيجابياً أو المغلوطة سلبياً. وفي نُظْم تقصي الإرهابيين، يكون الإبذار كاذباً إيجابياً عندما تُنذر خطأً عن شيء بريء بوصفه خطيراً. ويحدث الإبذار الكاذب السلبي عندما تفشل النُظْم في توقع حدوث ضربة إرهاب. ومن المستطاع ضبط النُظْم بما يزيد إمكان صدور إبذارات كاذبة إيجابياً (وحيثما تضبط النُظْم كي لا تترك أي شيء من دون الاشتباه فيه)، أو لزيادة تلك النسبة، بمعنى ضبط النُظْم كي تعطي عدداً أقل من الإبذارات الكاذبة إيجابياً لكن على حساب زيادة احتمال الفشل في تقصي هجمات إرهابية.

ولأن الضربات الإرهابية نادرة عددياً، تؤدي زيادة عدد الإبذارات الكاذبة إيجابياً إلى إرهاق نظام ملاحقة الإرهابيين برمتهم، مهما كانت الدقة في ضبط النُظْم⁽¹⁴⁾. وأنا استعمل كلمة «برمتهم» عامداً، للإشارة إلى أن ملايين الأشخاص سوف يتهمون خطأً عند اكتشاف أي مخطط إرهابي، بافتراض أن النُظْم تمكّنت من ذلك⁽¹⁵⁾.

ربما نستطيع التعامل مع حال يوضع فيها ملايين الناس في خانة الاشتباه، لو كانت تكلفة الإبذار الكاذب إيجابياً متدنية. ففكر بالمساحات الضوئية التي تمر فيها أجساد الناس في المطارات. إنها تصدر دوماً إبذارات إيجابية كاذبة، لكن الأمر لا يتطلب سوى أن يربت المفتش على المسافر كي يعرف الخطأ. لا يسير الأمر على ذلك النحو بالنسبة لنُظْم تقصي الإرهاب التي يشمل عملها الناس عموماً. إذ يتطلب كل إبذار إيجابي كاذب إنجاز تحقيقات مطوّلة لتحديد مصداقيته. يقتضي ذلك إنفاق

كثير من الجهد والوقت، ويعيق المحققين عن إنجاز أعمال أكثر جدوى. ويقول آخر أشد وقعاً، إذا كنت تراقب كل شيء فلن ترى شيئاً.

كذلك يتداول مجتمع الاستخبارات الأميركية تشبيهاً عن مخططات الإرهاب هو البحث عن إبرة في كومة قش. ووفق كلمات المدير السابق لـ «وكالة الأمن القومي» كيث ألكسندر، «أنت تحتاج إلى كومة قش كي تبحث فيها عن إبرة». تعبر تلك الجملة بالضبط عن مشكلة الرقابة العامة والتجميع الضخم للمعلومات. عندما تبحث عن إبرة في كومة قش، فإن آخر ما تتمناه هو إضافة مزيد من القش على الكومة⁽¹⁶⁾. يقول أكثر تحديداً، ليس من مبرر علمياً للاعتقاد بأن صبّ مزيد من البيانات العشوائية عن الناس، يزيد في سهولة اكتشاف مخططات الإرهاب، وهناك شواهد كثيرة على ذلك. إذ ربما ضمت تلك المعلومات إشارة ذات دلالة، لكن مقابل ذلك فإنها تضيف كثيراً من التشوش⁽¹⁷⁾. وعلى الرغم من عقلية «لنجمع كل شيء» السائدة في «وكالة الأمن القومي»، فإن وثائقها بالذات تدحض جدوى ذلك التفكير. أكثر من ذلك، يتحدث مجتمع الاستخبارات العسكرية عن «الشرب من أنبوب النار»، بمعنى الحصول على كميات ضخمة من المعلومات المفتقدة إلى الدلالة، مع ضياع تلك التي تحمل دلالة فعلياً⁽¹⁸⁾.

تبدت تلك النقطة في برنامج «وكالة الأمن القومي» للتنصت الإلكتروني، إذ فاقت الإنذارات الكاذبة إيجابياً القدرة على التعامل معها. في سنوات ما بعد 9/11، قدّمت «وكالة الأمن القومي» آلاف التلميحات إلى الـ «إف بي آي» شهرياً، لكنها كانت إنذارات إيجابية كاذبة⁽¹⁹⁾. كانت تكلفة ذلك الحال ضخمة، وانتهى الأمر إلى إحباط ضباط الـ «إف بي آي» الذين أجبروا على تقصي كل دليل محتمل. ظهر الأمر عينه في قاعدة البيانات المسماة «تقارير النشاطات المشتبه فيها» (Suspicious Activities Reports) التي جمعت عشرات آلاف التقارير لكنها لم تعط نتائج فعلياً⁽²⁰⁾. ولم تؤد كل الـ «ميتاداتا» التي جمعتها «وكالة الأمن القومي» إلا إلى نجاح يتيّم⁽²¹⁾: اعتقال سائق سيارة أرسِل 8500 دولار إلى تنظيم في الصومال لا يمثل

تهديداً مباشراً لأمن الولايات المتحدة. وجرى التطييل والتزوير لذلك الإنجاز، ربما لإعطاء «وكالة الأمن القومي» فرصة تسجيل نقاط في حوارها مع الكونغرس⁽²²⁾.

تمثل الفريدة التي تتمتع بها مخططات الإرهاب القضية الثانية التي تعيق استعمال تقنية التنقيب في المعلومات لمحاولة الكشف عن مخططات إرهابية⁽²³⁾. من كان يدري أنّ طنجرتيّ ضغطتصبحان قنبلتين محمولتين في حقيبتني ظهر لطالين جامعيّين في بوسطن، هما شاب وأخوه الكبير؟ كلما نفّذ شخص يندر توقع انخراطه في الإرهاب هجمة ما؛ فإنّه يولّد أثراً أضخم مما نفّذه عملياً بالنسبة للمعايير المعتمدة في توقع الأشخاص الذين يحتمل أن يكونوا إرهابيين، فتختل استراتيجيات ترصد الإرهابيين.

تظهر القضية الثالثة المعيقة للاستفادة من تقنية التنقيب في البيانات للكشف عن مخططات إرهاب، في أن الأشخاص الذين تلاحقهم «وكالة الأمن القومي» يتّسمون بالمرأوخة، ويسعون إلى التملّص من تتبع نشاطاتهم على الإنترنت. في عوالم التسويق المشخصن، لا يسعى الشخص عادة إلى إخفاء نشاطاته على الإنترنت. ولا ينطبق ذلك الوصف في سياق عمل الشرطة والأمن القومي. تؤدّي تلك العلاقة التصارعية [بين الأجهزة الأمنية والإرهابيين المحتملين على الإنترنت] إلى جعل الأمور أشد صعوبة، ما يعني أن معظم أدوات تحليل «البيانات الضخمة» المتوفرة في السوق لا تستطيع التعامل مع أحوال الإرهاب. إذ يمكن لأدوات السوق أن تتجاهل ببساطة الأشخاص الذين يتهربون منها، إضافة إلى أنها تفترض سلوكاً حميداً من قبل بقية الأفراد كافة. ولا تستطيع الأدوات التي تستخدمها الحكومة في تحليل البيانات تبني تلك المقاربة؛ لأنها تسعى بالضبط إلى التقاط الأشخاص المرأوخين.

يتفاوت أولئك الأعداء في مدى تقدّم قدرتهم على تجنّب الرقابة. ولا يمتلك معظم المجرمين والإرهابيين - وكذلك الحال بالنسبة للمنشقين سياسياً، وهو

أمر من المؤسف قوله - تمرساً كافياً في التملص من الرقابة الإلكترونية، ولذا فهم يرتكبون أخطاء جمة. ولا يصلح ذلك تبريراً للجوء إلى تقنية التنقيب في المعلومات، خصوصاً أن الرقابة الموجهة تستطيع الوصول إليهم. يجدر السؤال عن الفارق بين الرقابتين العامة والموجهة في الوصول إلى أولئك الأشخاص، وإذا كان الفارق يبرر الأكلاف العالية المتصلة بالرقابة العامة. وأظهرت مجموعة من التحليلات لجهود «وكالة الأمن القومي» أن الأمر ليس كذلك أبداً⁽²⁴⁾.

إذاً، لا يمكن إصلاح القضايا الثلاث التي أثرت آنفاً. ببساطة، يشكل التنقيب في البيانات أداة من الخطأ استعمالها لتقصي الإرهابيين، ما يعني أنه لا يمكن تبرير فرض رقابة عامة⁽²⁵⁾. وعندما كان مدير آل «وكالة الأمن القومي»، حاجج كيث ألكسندر بأن الرقابة الشاملة كانت كفيلة بتمكين الوكالة من اكتشاف مخططات 9/11⁽²⁶⁾. لا يبدو ذلك أمراً مرجحاً. إذ لم يتمكن ألكسندر من درء تفجيرات «ماراثون بوسطن» في 2013، على الرغم من أن أحد المفجرين كان موجوداً على لائحة المراقبة الخاصة بالإرهابيين، وترك المفجران آثاراً كبيرة تتصل بمخططيهما في وسائط التواصل الاجتماعي⁽²⁷⁾. وحدثت تلك التفجيرات بعد ما يزيد على عشر سنوات من 9/11، حدثت فيها قفزات كبرى في التقنيات المتصلة بالرقابة. وكانت لدى «وكالة الأمن القومي» معلومات جمة عن الإخوة تسارنايف قبل تنفيذهما تفجيرات «ماراثون بوسطن»، لكن الوكالة لم تلاحظ فارقاً بين تلك المعلومات وما جمعتها عن ملايين الناس⁽²⁸⁾.

أثيرت تلك النقطة ضمن تقرير لجنة التحقيق في 9/11 الذي تحدّث عن الفشل «في توصيل النقط»، الذي يرى فيه مؤيدو الرقابة العامة مبرراً لجمع كميات من المعلومات تتزايد باطراد. ولاحظ التقرير أن مجتمع الاستخبارات الأميركي استطاع تجميع معلومات عن ذلك المخطط، من دون اللجوء إلى الرقابة العامة، متنبهاً إلى أن الفشل تأتي فعلياً من التحليل غير المناسب للمعلومات⁽²⁹⁾.

لم تستطع الرقابة الشاملة الإمساك بالملابس الداخلية للمُفجّر عمر فاروق عبد المطلب في 2006، على الرغم من أنّ أباه حذّر الحكومة الأميركية تكراراً من كون ابنه خطيراً⁽³⁰⁾. وفي العام 2006، عُثر على المتفجّرات السائلة⁽³¹⁾ - وهي الحجة التي تستخدمها الحكومات في منع المسافرين جواً من وضع زجاجات كبيرة من السوائل والكريمات وال «جيل» في حقائب اليد التي يحملونها معهم إلى الطائرة - في شقّة في لندن جرى تحديدها بفضل تحقيق بوليسي بوسائل تقليدية، وليس بواسطة رقابة عامة. وفي الحالات المعروفة عن نجاح «وكالة الأمن القومي»، كانت المعلومات تأتي دوماً من الرقابة الموجهة، وليس برقابة عامة⁽³²⁾. ويبيّن أحد التحليلات أنّ الـ «إف بي آي» تتعرّف إلى مخططات إرهابية محتملة بواسطة تقارير عن النشاطات المشبوهة⁽³³⁾، وتقارير عن مخططات لارتكاب جرائم أخرى، وكذلك من التحقيقات المتعلقة بتلك الجرائم.

إنّها نقطة حاسمة. إذ لا تمثّل الرقابة الشاملة ولا تقنية التنقيب في المعلومات أدوات مناسبة للعثور على إرهابيين ومجرمين. وتُبدّد بلايين من دولارات دافعي الضرائب على برامج الرقابة العامة، من دون الحصول على الأمن الذي تعدنا به. وهناك ما هو أشد أهمية من ذلك، بمعنى أن الأموال تُبدّد على تلك البرامج اللامجدية للرقابة العامة، بدل إنفاقها على التحقيق والاستخبارات والاستجابة للحالات الطارئة؛ وكلها تكتيكات أثبتت جدواها⁽³⁴⁾.

تصلح الرقابة العامة وتقنية التنقيب في البيانات في مهمات تتعلق بالتمييز بين عموم الناس، بمعنى العثور على أصحاب ميول سياسيّة معيّنة، وأولئك الذين يصادقون شخصيات بعينها، والأعضاء في جمعيات سرية، والأفراد الذين يرتادون لقاءات وتظاهرات محدّدة. يكون أولئك الناس موضع اهتمام حكومات تميل للسيطرة على المجتمع، كالصين. ويرجع سبب نجاعة استخدام تقنية التنقيب في المعلومات في كون المنشقّين سياسياً، على غرار مزوّري بطاقات الائتمان؛ يتشاركون بصورة عامة في بروفايلات محدّدة. ويضاف إلى ذلك أنّ الحكم المتسلّط لا يكثر

لمسألة الإنذارات السلبيّة الكاذبة؛ لأن إدانة البريء بتهمة التحريض على العصيان ينشر الخوف في قلوب العامة.

وإضافة إلى كونها غير فعّالة، فإن الرقابة العامة التي تمارسها «وكالة الأمن القومي» تجعلنا عملياً أقلّ أمناً. ولتبيان جليّة ذلك الأمر، يجب عليّ أن أتوسّع قليلاً في شرح أمن الإنترنت ومسألة التشفير ونقاط الضعف في نُظُم الكمبيوتر. وتبين المقاطع الثلاثة التالية تلك الأمور، ما يجعلها مقاطع مهمة أيضاً.

الهجوم مقابل الدفاع في الإنترنت

في الأوضاع الأمنيّة كافة، يحدث سباق في التسلّح بين الهجوم والدفاع. يكسب أحد الطرفين السباق لفترة ما، ثم تتبدّل التقيّة ويكسب الطرف الآخر تفوّقاً، ثم تتغيّر الأحوال كرة أخرى.

فكّر في تاريخ التقنيّات العسكريّة وتكتيكاتها. في مطالع القرن التاسع عشر، مالت الكفّة لمصلحة المياليّن إلى الأساليب الدفاعيّة؛ ذلك أن تحطيم خط دفاعي كان أكثر كلفة من حمايته. كان نابليون بونابرت سباقاً في التفكير في أساليب الهجوم الفعّالة مع استخدام الأسلحة التي كانت متوفّرة في ذلك الوقت. ومع الحرب العالميّة الأولى، حازت الأسلحة الناريّة - خصوصاً الرشاشات الثقيلة - حدّاً كبيراً من القوّة، فمالت الكفّة مجدّداً صوب الأساليب الدفاعيّة؛ لأن أسلحة المتحصنين كانت قميّنة بحصد المهاجمين. وانقلبت موجة المدّ ثانية في الاتجاه المعاكس مع الحرب العالميّة الثانية، مع التسليح المتطوّر للدبابات والمدرّعات الميكانيكيّة، ما أعاد الأفضليّة إلى أساليب الهجوم.

وحاضراً، يمتلك المهاجم الأفضليّة على شبكة الإنترنت ونُظُم الكمبيوتر عموماً⁽³⁵⁾. وهناك أسباب تفسّر ذلك:

* يسهل تحطيم الأشياء ولكن يصعب إصلاحها⁽³⁶⁾.

* يعدُّ التعقيد العدو الأسوأ للأمن، وتسير نُظم المعلوماتية بأطراد نحو مزيد من التعقيد⁽³⁷⁾.

* تسهّل طبيعة نُظم الكومبيوتر للمهاجم العثور على نقطة ضعف قابلة للاستغلال، فيما يجب على المدافع معرفة نقاط الضعف كلها ثم العمل على إصلاحها.

* يستطيع المهاجم أن يختار هجمة ما ويركّز جهوده عليها، فيما يفترض بالمدافع أن يتحسّب لأنواع الهجمات كلها.

* غالبية البرامج الرقمية ضعيفة أمنيّاً⁽³⁸⁾. وببساطة، ليس من السهل كتابة برامج آمنة، وإنشاء نُظم كومبيوتر آمنة. نعم، هناك تطوّر يحدث باستمرار في ذلك الصدد، لكن الأمر لم يصل بعد إلى المستوى المطلوب.

* الأمن المعلوماتي هو شأن تقني معقّد، ومن السهل أن يقع المستعمل العادي في الخطأ، فيخرب ما صُنّع لحمايته.

ليس من السهل القول إنّه لا جدوى من أمن الإنترنت، لأن الأمر بعيد عن ذلك. فعلى الرغم من سهولة الهجوم، فإن الدفاع ما زال ممكناً. إذ تتكفّل الحماية الجيّدة بجعل الهجمات أشد صعوبة، وأعلى كلفة وأشد خطورة على منفذها. وإذا لم يكن المهاجم متمرساً، يستطيع الأمن المعلوماتي توفير حماية كاملة منه.

في حقل الأمن، يتمحور التفكير حول إدارة المخاطر. ويجب أن تعرف ما الخطر الذي تواجهه، وما هو الأسلوب العقلاني في التحوّط منه. وبالنسبة لكل من لديه كومبيوتر في المنزل، يجب الحصول على برنامج جيّد في الأمن المعلوماتي، والحرص على الاستفادة دوماً من التجديدات، وتجنّب المواقع الشبكية المشبوهة، وتفادي قراءة مرفقات الرسائل الإلكترونية الآتية من أشخاص مجهولين، والحرص على الاحتفاظ بنسخ احتياطية. تستطيع تلك الخطوات وغيرها من الإجراءات الأمنية الأساسية

أن تجعلك منيعاً حيال مجرمي الإنترنت العاديين والـ «هاكرز» غير المتمرسين. من ناحية أخرى، إذا كنت منشقاً سياسياً في الصين أو سوريا أو أوكرانيا، وتحاول تجنب الاعتقال أو الاغتيال؛ يجدر بك اللجوء إلى إجراءات حماية أكثر شمولاً واتساعاً. وتنطبق النصائح السابقة عليها إذا كنت مجرماً تحاول التهرب من الشرطة، أو رجل أعمال يحاول منع تجسّس الشركات الأخرى على أعماله، أو سفارة رسمية تسعى إلى صد التجسّس العسكري عليها. وإذا كان لديك قلق خاص تجاه المعلومات التي تجمعها الشركات عنك، فلسوف تحتاج إلى مجموعة أخرى من إجراءات الأمن المعلوماتي.

بالنسبة لعدد من الشركات، تُردّ مسألة الأمن إلى الحسابات الأساسية اقتصادياً. إذا كانت تكلفة الأمن أقل من الخسائر الناجمة عن غيابها، تميل الكفة إلى الأمن. إذا فاقت تكلفة الأمن ما تحدّثه الهجمات من خسائر، يكون الحل في تقبّل الخسائر. بالنسبة للأفراد، هناك كثير من المزج بين البعد النفسي والاقتصادي. إذ يصعب احتساب الكلفة المادية الناجمة عن فقدان الخصوصية، أو من وضع أسماء الأفراد على لوائح المراقبة. وعلى الرغم من ذلك، تبقى المعادلة على حالها: الكلفة مقابل الاستفادة.

من الأهمية بمكان في هذا التحليل ملاحظة الفارق بين الهجمات العشوائية والموجّهة.

تتسم غالبية الهجمات الإجرامية بالانتهازية. في العام 2013، دخلت مجموعة من الـ «هاكرز» إلى الشبكة الداخلية لسلسلة محلات «تارغت» للبيع بالتجزئة، وسرقوا معلومات عن 40 مليون شخص تتعلق ببطاقات الائتمان وبيانات شخصية متنوعة⁽³⁹⁾. وحينها، وُصِفَ ذلك الاختراق بأنّه الأضخم، وتسبّب بكارثة للشركة⁽⁴⁰⁾ استقال إثرها مديرها التنفيذي، كريغ شتاينهافل⁽⁴¹⁾؛ لكن المجرمين لم يختاروا استهداف «تارغت» تحديداً لأي سبب أيديولوجي. إذ انصب اهتمامهم

على أرقام بطاقات الائتمان كي يتمكنوا من تزويرها؛ وكانوا ليفعلون الأمر نفسه مع أي شركة أخرى. لو امتلكت «تارغت» نظاماً أشد متانة في الأمن المعلوماتي، لتوجه المجرمون إلى شبكات أخرى. يشبه أمرهم أمر السارق التقليدي للبيوت. إذ هو يسعى إلى سرقة بيت، ولربما كانت لديه خيارات بالنسبة لنوعية البيوت والأحياء، لكنه لا يكثرث للبيت الذي يتمكن من سرقة. وتمثل مهمتك كمالك للبيت في جعل منزل أقل إغراءاً للسارقين من المنازل المجاورة لك. وللتصدي لهجمات غير موجهة، يكون الأمن الجيد مسألة نسبية.

قارن ذلك مع هجمات العام 2012 على صحيفة نيويورك تايمس من قبل «هاكرز» صينيين ربما كانوا على صلة بحكومة بلادهم⁽⁴²⁾. في تلك الحال، سعى المهاجمون إلى ترصد اتصالات مراسلي الصحيفة مع منشقين صينيين. واستهدفوا تحديداً البريد الإلكتروني لنيويورك تايمس وشبكاتها الرقمية الداخلية؛ لأنها الأمكنة التي تحتوي على المعلومات التي يسعون إليها. في حال الهجمات الموجهة، ما يصنع الفارق هو المستوى المطلق للأمن. لا يتعلق الأمر بأن سرقة جارك ربما تكون أسهل؛ لأن المهاجم يستهدفك تحديداً، ما يعني وجوب أن تمتلك قدرات دفاعية تستطيع التصدي لإمكانات من يهاجمونك تحديداً.

هناك مثل آخر على ذلك الأمر. يعرف عن شركة «غوغل» أنها تسمح بانتظام بريد «جي ميل» الإلكتروني، وتستخدم المعلومات التي تحصدها في توجيه الإعلانات إلى الجمهور. بالطبع، لا يجري ذلك على يد موظف بعينه في «غوغل»، بل تنهض الحواسيب بتلك المهمة. لذا، فإذا كتبت بريدك الإلكتروني بلغة غير مألوفة لا يستطيع «غوغل» ترجمتها أوتوماتيكياً، سوف تكون في مأمن من المسوحات التي يجريها «غوغل» باستخدام جداوله الخوارزمية الخاصة؛ فليس مجدياً لتلك الشركة أن تترجم يدوياً رسائلك الإلكترونية. لكن، إذا صرت فجأة هدفاً لتحقيق موجه يجريه الـ «إف بي آي»، سوف يخصص المحققون وقتاً للترجمة اليدوية للرسائل الغامضة في بريدك الإلكتروني.

تذكر دوماً هذا الفارق الأمني بين الرقابة العامة والرقابة الموجهة؛ لأننا سنعود مراراً وتكراراً إليه.

قيمة التشفير

قدّمت الكلمات السابقة وصفاً لأمن الإنترنت كنوع من سباق التسلّح يمتلك فيه المهاجم أفضلية على المدافع. ربما تكون الأفضلية كبيرة، لكن يبقى أن لها حدوداً. لا يكون الأمر أبداً أن طرفاً ما يحوز تقنية فائقة القوة إلى حدّ أن الطرف الآخر لا يستطيع الانتصار عليها، على خلاف ما يظهر في الأفلام والكتب المصوّرة.

التشفير، بل كتابة الشيفرة عموماً، هو استثناء. لا يقتصر الأمر على كون الدفاع أشد سهولة من الهجوم، بل إنه أكثر سهولة إلى حدّ أن الهجوم يغدو مستحيلاً بصورة أساسية.

ثمة أفضلية رياضية بنيوية متأصلة بين كتابة الشيفرة، بالمقارنة مع محاولة كسر التشفير. أساساً، يستند الأمن المعلوماتي إلى طول مفاتيح الشيفرة، وإذا حدث أضال تغيير في طول المفتاح، فسيفرض ذلك على المهاجم عملاً إضافياً فائق الضخامة. وتتضخم تلك الصعوبة بما يشبه الانتقال من رفع العدد إلى قوة 2 ثم 3 ثم 4 وهكذا دواليك. ربما يستغرق المهاجم يوماً كي يكسر مفتاحاً من 64 بايت، لكنه يحتاج ضعفي ذلك الوقت إذا زاد طول المفتاح إلى 65 بايت. وعند صنع مفتاح من 128 بايت، يتطلّب ذلك ضعفي الزمن في كتابة الشيفرة، يحتاج المهاجم إلى زمن أطول بمقدار الضعفين مرفوعاً إلى قوة 264، ما يساوي مليون بليون سنة من العمل الإضافي لكسر تلك الشيفرة. (للمقارنة، يبلغ عمر الكرة الأرضية 4.5 بليون سنة).

لذا تسمع عبارات من نوع «سوف يستغرق كسر هذه الشيفرة زمناً يساوي استنفاد طاقة الحرارة من الكون بأكمله، حتى لو افترضنا أن المهاجم صنع كومبيوترا باستخدام الذرات الموجودة في الكرة الأرضية بأكملها».

يصح قول ذلك نظرياً على الأقل. المشكلة أن الشيفرة هي حزم من المعادلات الرياضية، لكن الرياضيات لا وكالة لها. عند السعي إلى تحويل تلك المعادلات الرياضية إلى شيء يمنحك بعض الحماية، يتطلب الأمر كتابة ذلك بواسطة شيفرة الكمبيوتر. كذلك يجب أن تُفعل تلك الشيفرة على الكمبيوتر الذي يحتوي أجهزة ومكونات إلكترونية صلبة، ويعمل بنظام تشغيل، كما يحتوي على برامج متنوعة. كما يفترض أن يدير شخص ما ذلك الكمبيوتر الذي يفترض توصيله بشبكة رقمية أيضاً. وتتكفل تلك الأشياء جميعها بإدخال عناصر الهشاشة إلى الشيفرة، ما يهزّ التكامل الذي تأتي لها من معادلات الرياضيات. ويعود ذلك بنا إلى نقاش حال الأمن التي عرضناها من قبل، وهي منحازة بشدة للمهاجم.

بالأكيد، تملك «وكالة الأمن القومي» بعض الرياضيات السرية مع قدرات هائلة في الحوسبة، ما يمكنها من كسر بعض أنواع التشفير بسهولة نسبية. وكذلك بنّت «مؤسسة البحوث المتعددة البرامج» في «أوك ريدج» بولاية تينيسي، لتلك الغاية⁽⁴³⁾. ولكن، مهما كانت قدرات التشفير وكسره متقدمة في «وكالة الأمن القومي»، فإن وثائق سنودن تظهر أنها تستفيد بشكل واسع من نقاط ضعف وهشاشة لدى آخرين - كأن يكونوا أشخاصاً أو حواسيب أو شبكات - للالتفاف على التشفير، بدل الاصطدام به مباشرة. تخترق «وكالة الأمن القومي» النظم الإلكترونية، وهو عين ما يفعله مجرمو الإنترنت. وكذلك ألقت مجموعة محترفة اسمها «عمليات النفاذ المرسومة»، تتولى اختراق الشبكات وسرقة مفاتيح التشفير. وكذلك تستغل الوكالة كلمات المرور السيئة التركيب، والمفاتيح الضعيفة وتلك المعرفة سلفاً من قبل النظام الإلكتروني الذي تسعى إلى اختراقه. وخلصه، تدس الوكالة شفيرات ضعيفة في المنتجات الإلكترونية والرقمية، بما فيها البرامج الرقمية والمعايير الإلكترونية⁽⁴⁴⁾.

في العام 2013، صاغ سنودن ذلك في حوار على الإنترنت على النحو التالي: «التشفير مفيد عملياً. وإذا نُفذ بطريقة ملائمة، يكون باستطاعتك الاعتماد على

نظام جيد التشفير. ولسوء الحظ، فإن الأمن عند نقاط التقاطع بين التشفير والنظم والأدوات يكون هشاً بصورة مريعة، ما يمكن «وكالة الأمن القومي» من الالتفاف حوله دوماً»⁽⁴⁵⁾.

وفي المقابل، تبين الطرق الأخرى التي تلجأ إليها الوكالة لضرب التشفير مدى أهميته. وعندما يتمكن التشفير من التوصل إلى تعديل الكفة في الرياضيات، يُجبر المهاجم على اللجوء إلى طُرُق أخرى. وبدلاً من التنصت بسكون على أقتية الاتصالات وجمع المعلومات عن الجميع، ربما وجب على المهاجم اختراق نظام كومبيوتر معين وسرقة النصوص مباشرة. تفرض تلك الطُرُق في الالتفاف حول التشفير بذل جهد أكبر، والتعرض لمخاطر أكثر، وزيادة التضيق في الاستهداف، بالمقارنة مع ما يكونه الحال عند جمع معلومات غير مشفرة.

لتذكر المبادئ الاقتصادية لـ «البيانات الضخمة» وهي: من الأسهل تجميع كل شيء بدل التفكير فيما يجب جمعه أو تركه، ومن الأسهل التجسس على الجميع بدل التفكير في فرز من يستأهل التجسس عليه. ويتكفل انتشار التشفير بجعل عمليات الرقابة العامة غير مجدية، كما يفرض أن يقتصر التنصت على أهداف متقاة. وفي تلك الحال، تحقق الخصوصية مكسباً كبيراً؛ لأن المهاجم لن يمتلك أبداً ميزانية تكفي لجعل الجميع أهدافاً متقاة.

الثغرات وانتشارها

الثغرات أخطاء. أخطاء في تصميم النظم الإلكترونية أو تنفيذها - هنات في الشيفرة أو المكونات الإلكترونية الصلبة - يتيح الدخول غير المصرح به إلى النظام. بوسع مجرم في الفضاء السبراني، مثلاً، استغلال ثغرة ما ليدخل إلى حاسوبك، أو يتنصت على اتصالاتك الشبكية، أو يسرق كلمة المرور التي تستعملها في الدخول إلى حسابك البنكي. وربما يتمكن موظف حكومي أمني من استعمال ثغرة ما لاختراق شبكة منظمة إرهابية أجنبية وإجهاض عملياتها، أو سرقة الملكية الفكرية لشركات

أجنبية. وربما يستغل موظف آخر ثغرة ما للتنصت على منشقين سياسيين، أو خلايا إرهابية، أو قادة حكومات معادية. كذلك قد يستغل الجيش ثغرة ما لشن حرب في الفضاء الافتراضي. تندرج تلك الأفعال كلها تحت تصنيف الاختراق الإلكتروني.

عندما يكتشف المرء ثغرة معينة، يستطيع استعمالها للدفاع أو الهجوم. ويُترجم الدفاع بالاتصال بالشركة البائعة وتنبهها إلى الثغرة كي تعالجها وتسدها، وكذلك نشرها كي يتمكن المجتمع من التعلم منها. يجري التعرف إلى ثغرات كثيرة من قبل الشركات البائعة، وتعتمد إلى معالجتها من دون إثارة ضجيج حولها. ويحدث التعرف إلى هشاشات أخرى على يد الباحثة والـ «هاكرز» الأخلاقيين.

يترجم الهجوم باستغلال الثغرة لشن هجمات على آخرين. ويطلق على الثغرات غير المعلن عنها تعبير «ثغرات اليوم صفر»، بمعنى أن قيمتها تأتي من كونها ثغرات تمنح المهاجم فرصة شن هجمات لا يملك أحد دفاعاً ضدها. وبذا، يكون من المستطاع شن هجمات عالمية مع الإفلات من العقاب. وفي نهاية الأمر، سوف تكتشف الشركة الصانعة ثغرة ما- ويعتمد وقت حدوث الاكتشاف على المدى الذي استُغِلَّت به الثغرة- ثم تصدر برنامجاً لسد تلك الثغرة.

إذا كان المهاجم المكتشف للثغرة مجموعة عسكرية أو شركة لصنع الأسلحة، فلسوف تُبقي أمرها سراً كي تبني سلاحاً سبرانياً يستند إلى تلك الثغرة. وإذا جرى استغلالها لمرات نادرة وبسريرة مناسبة، فلنما تبقى طويلاً طي الكتمان. وإذا لم تستعمل إطلاقاً، فستبقى سراً إلى أن يكتشفها طرف آخر.

يستطيع مكتشفو الثغرات بيع معلوماتهم عنها⁽⁴⁶⁾. هناك سوق قوي للأسلحة السبرانية المناسبة لـ «اليوم صفر»⁽⁴⁷⁾ - يتمثل الشراء فيه بالحكومات والشركات التي تصنع الأسلحة السبرانية وتبيعها للحكومات⁽⁴⁸⁾ - إضافة إلى سوق سوداء يبيع فيها مكتشفو الثغرات المعلومات لمجرمين⁽⁴⁹⁾. هناك شركات تمنح مكافآت

لمن يكتشف ثغرات في منتجاتها بهدف تحفيز البحوث الدفاعية، لكن الجوائز تبقى أقل مما يمكن تحصيله من بيعها.

من الأمور الشائعة وجود ثغرات تصلح في «اليوم صفر». إذ تحتوي كل قطعة من البرامج الرقمية التجارية - في هاتفك الخليوي، وحاسوبك المنزلي، والنظم التي تدير المفاعلات الذرية - مئات بل آلاف من الثغرات معظمها غير مكتشف⁽⁵⁰⁾. يرجع ذلك إلى أن علم البرمجة ليس على قدر من التطور كي يعطي برامج خالية من العيوب كلياً، وليس من المتوقع أن يتغير ذلك الأمر قريباً. وتعطي اقتصاديات صنع البرمجيات الرقمية الأولوية إلى السرعة والميزات الجذابة، وليس للأمن⁽⁵¹⁾.

المعنى المقصود من الكلام هو أن الاختراق لن يختفي. في المستقبل المنظور، سيكون من المستطاع دوماً أن يكتشف مهاجم متمرس تقنياً ثغرة كي ينفذ منها إلى نظام المدافع. ويصح ذلك أيضاً بالنسبة للجيش التي تصنع أسلحة سبرائية، ووكالات الاستخبارات التي تحاول اختراق النظم الإلكترونية بهدف التنصت، وكذلك المجرمين من الأنواع كافة.

الحفاظ على إنترنت غير آمنة

في الفصل الأول، بينتُ أن «وكالة الأمن القومي» تخترق النظم الإلكترونية باستخدام ثغرات موجودة، وأخرى يجري اصطناعها لتلك الغاية. وفي أفعال الوكالة، تتقدم الرقابة على الأمن، ما يؤول إلى وضع نكون فيه جميعاً أقل أماناً. ويبيّن مقال عن وثائق سنودن نشرته صحيفة الغارديان البريطانية طريقة تفكير «وكالة الأمن القومي» ونظيرتها البريطانية «القيادة الحكومية للاتصالات»⁽⁵²⁾. ويورد المقال: «هناك ملخصات متبادلة بين الوكالتين تظهران احتفالهما بهزيمة الأمن والخصوصية على الشبكة...».

كيف تقهر الحكومات الأمن والخصوصية معاً؟ بتنا نعرف أن «وكالة الأمن القومي» تستخدم 4 ممارسات رئيسية في عملها⁽⁵³⁾. والأرجح أن دولاً كروسيا والصين وبلدان أخرى تفعل أموراً مشابهة. وليس مجرمو الإنترنت ببعيدين عن ذلك أيضاً.

تعتمد الوكالة إلى مراكمة الثغرات في البرامج الرقمية التجارية التي نستخدمها يومياً، بدلاً من سعيها للتأكد من إصلاح تلك الأخطاء. عندما تكتشف «وكالة الأمن القومي» (أو تشتري) ثغرة ما، فإنها تستطيع إما أن تنبئ الشركة البائعة لتلك البرامج مع إصلاح تلك الثغرة غير المعروفة، أو تتمسك بتلك الثغرة كي تكون منفذاً لها للتنصت على نظم كومبيوتر تسعى الوكالة إلى استهدافها. ويخدم التكتيكان كلاهما أهدافاً مهمة في سياسة الولايات المتحدة، لكن يجب على الوكالة في كل مرة أن تختار سلوك أيّ من الطريقتين.

حاضراً، تملك الولايات المتحدة - «وكالة الأمن القومي» والحكومة معاً - أعداداً متراكمة من ثغرات «اليوم - صفر»؛ ليس معروفاً عددها. في العام 2014، حاول البيت الأبيض توضيح ذلك الأمر بواسطة مُدوِّنة إلكترونية، لكن ما قدّمه لم يكن شرحاً كافياً⁽⁵⁴⁾. نعرف أن سلاحاً سبرانياً هو فيروس «ستاكس نت»، استخدم ذخيرة من ثغرات «اليوم - صفر» تكفي أربعة أيام من الحرب السبرانية⁽⁵⁵⁾. ويؤشّر استخدام ذلك العدد في شنّ هجمة سبرانية مفردة على وجود ذخيرة لمئات الأيام في مخازن الحكومة.

في شهادته أمام الكونغرس، قدّم مايكل هايدن، المدير السابق لـ «وكالة الأمن القومي» تعريفاً لمصطلح متداول في أوساط الوكالة هو «نوباس» (NOBUS)⁽⁵⁶⁾ الذي يتألف من الحروف الأولى لعبارة «لا أحد سوانا» بالإنكليزية (no body but us) - وهي إشارة إلى اكتشاف ثغرة يرجح ألا يعرفها أحد سوى الوكالة. تملك الوكالة آلية سرية كي تقرّر ما يجب فعله بصدد الثغرات. إذ تزعم الوكالة أنها

تعلن وتسدّ معظم ما تكتشفه من ثغرات⁽⁵⁷⁾، لكنها تحتفظ ببعضها - وعددها غير معروف - عندما تتوصل إلى قناعة بأنها ثغرة من نوع «نوباس».

تبدو تلك المقاربة كأنها تصلح إطاراً عاماً، لكنها تصبح صعبة عند التطبيق. من يعمل في حقل الأمن يعي صعوبة اتخاذ قرارات من نوع «نوباس»، بل ربما لا تستطيع الحكومة ذلك أيضاً⁽⁵⁸⁾.

تحمل تلك السجلات المترامية للثغرات تهديداً للجميع. إذ تجمعنا الثغرات المفتوحة أقل أمنًا، فلربما توصل أحد إلى معرفة إحداها واستخدامها في شنّ هجمات علينا. والأصل في تلك الثغرات أنها مزعومة للاستقرار⁽⁵⁹⁾، خصوصاً أنها لا تستمر طويلاً، فلا تحصل فائدة من مراكمة سجلات عنها والتفكير بأنها موجودة دوماً بتصرّفنا. والأنكى من ذلك كله أن كل استخدام لها يمتزج بخطورة أن يتنبّه آخرون لها ويستخروها لمصلحتهم. ولأن تلك الثغرات تأتي في أنواع مترافقة، فإن حفظ السرّ بشأن إحداها ربما يعني أن صنفاً بأكمله من الثغرات يبقى غير مكتشف، وتالياً لا يجري سدّه وإصلاحه. وكذلك تكون الولايات المتحدة والبلدان الأوروبية معرضة تماماً لتهديدات من نوع «اليوم - صفر»، بأثر من حساسية بنيتها التحتية الإلكترونية، والملكية الفكرية والثروات الشخصية. وتكون بلدان كالصين وروسيا أقلّ تعرّضاً لتلك المخاطر - وكوريا الشمالية أقلّ كثيراً -، لذا تتدنّى لديهم كثيراً الحوافز للتصدي للثغرات والعمل على إصلاحها.

تعمل «وكالة الأمن القومي» على زرع «أبواب خلفية» في مكونات الأجهزة الإلكترونية وبرامجها أيضاً. ليست «الأبواب الخلفية» شيئاً جديداً⁽⁶⁰⁾.

ولطالما أعربت شركات المعلومات والاتصالات المتطورة عن قلقها حيال تمكن الـ «هاكرز» من زرع «أبواب خلفية» في البرامج، كما بذلت جهوداً ضخمة في العثور عليها وإزالتها. وأخيراً، صرنا نعرف أن الحكومة الأميركية تعتمد زرع «أبواب خلفية» في الأجهزة الإلكترونية والبرامج الرقمية⁽⁶¹⁾.

إذ تبين إحدى وثائق سنودن تفاصيل مشروع لـ «وكالة الأمن القومي» يحمل اسم «مشروع تمكين سيغينت» (SIGINT Enabling Project) ⁽⁶²⁾ الذي يعتمد تكتيكات من قبيل «زرع ثغرات في نظم التشفير التجارية، ونُظم المعلوماتية، والشبكات الرقمية، والأجهزة الإلكترونية للاتصالات التي يستخدمها الجمهور». لا يُعرف الكثير عن ذلك المشروع، ولا عن مدى معرفته من قبل شركات صناعة المعلوماتية والاتصالات المتطورة وموافقتها عليه، وكذلك الحال بالنسبة للسرية التي تدس بها خلصة تلك الثغرات، سواء عبر موظفين في الشركات يعملون لمصلحة الحكومة أم بالتلاعب بطرق خفية بالشفيفرات الرئيسة للشركات. وكذلك نجهل مدى نجاح المشروع - إذ لم تورد وثائق سنودن تفاصيل كثيرة عن ذلك - لكننا بتنا نعرف أنّ ميزانيته هي 250 مليون دولار سنوياً. ولا نعرف أيضاً إذا كانت دول أخرى تفعل أشياء مشابهة بالنسبة للنُظم التي تنتجها شركات تقع تحت سيطرتها السياسية.

لكن بعض الأمثلة باتت معروفة. في الفصل 6، تحدّثُ عن تجاوب «مايكروسوفت» مع طلب «وكالة الأمن القومي» توهين شيفرة برنامج «سكايب». كذلك ضغطت الوكالة على «مايكروسوفت» لوضع «باب خلفي» في شيفرة برنامجها الذي يشغّل القرص الصلب «بيت لوكر» (Bit Locker) ⁽⁶³⁾. ومن المستطاع الافتراض بأن جهوداً أخرى طاولت منتجات أخرى، إذ تناهت إلى مسامعي بصورة شخصية بعض القصص عن إخفاقات في ذلك الصدد.

تحمل الثغرات المتعمدة مخاطر كبرى، فلا وسيلة للتأكد من أن «باباً خلفياً» دسّته الحكومة عمداً سوف يبقى حكراً عليها ⁽⁶⁴⁾. وتدفع ثغرات النفاذ المفروضة حكومياً بالشركات إلى جعل منتجاتها وخدماتها أقل أماناً بالنسبة للجميع ⁽⁶⁵⁾.

مثلاً، بين حزيران (يونيو) 2004 وآذار (مارس) 2005، تمكن أحدهم من تتبّع مكالمات قرابة 100 خلوي لموظفين في الحكومة اليونانية، بينهم رئيس الوزراء، ووزراء الدفاع والخارجية والعدل، إضافة إلى مواطنين يونانيين بارزين.

لقد صمّمت شركة «إريكسون» السويدية الشيفرة التي تمكّن من ذلك التتبّع في منتجات لشركة «فودافون»، لكنها لم تكن تُفعلها إلا للحكومات التي تطلب تلك المنتجات⁽⁶⁶⁾. لم تكن الحكومة اليونانية بين تلك الحكومات، لكنّ أحداً ما- ربما مجموعة سياسية مناوئة أو تنظيم إجرامي - تمكّن خفية من تفعيل تلك الميزة.

لم يكن ذلك حادثاً معزولاً. إذ حدث أمر مشابه في إيطاليا في 2006⁽⁶⁷⁾. في العام 2010، استفاد «هاكرز» صينيّون من ثغرة وضعها «غوغل» عمداً في بريد «جي ميل»، لتمكين الحكومة الأميركية من اعتراض الرسائل الإلكترونية في ذلك البريد⁽⁶⁸⁾. وفي 2012، ظهر إلى العلن أن كل محوّل للاتصالات التليفونية بيع إلى وزارة الدفاع، يحتوي ثغرات مبنوثة في نظامه للرقابة، لكن لم يكن واضحاً مدى التعمّد في ذلك الأمر⁽⁶⁹⁾.

باستمرار، تستفيد «وكالة الأمن القومي» من «أبواب خلفية» وضعتها بلدان أخرى في نُظُم إلكترونية، خدمة لأهداف أخرى⁽⁷⁰⁾. ومثلاً، استفادت الوكالة من قدرات في التتبّع وضعتها حكومة «برمودا» في نظامها الهاتفي، فتمكّنت الوكالة من تتبع المكالمات الهاتفية كافة في ذلك البلد⁽⁷¹⁾. لم نعتقد بأن ذلك لا يحصل للولايات المتحدة أيضاً؟

تعتمد الوكالة إلى تخريب الجداول الخوارزمية ومعايير التشفير. هناك هدف آخر لـ «مشروع تمكين سيغنت» يتمثّل في «التأثير في السياسات، والمعايير والنُظُم المُحدّدة لتقنيّات المفتاح العام التجاري في التشفير»⁽⁷²⁾. ومرة أخرى، لا تتوافر تفاصيل كثيرة عن تلك النشاطات، لكنني أتوقّع أنها تركز على المعايير المرسومة في براءات اختراعات، كتلك التي تحوزها شركات صنع الهواتف الخلوية، بأكثر من تركيزها على معايير عامة كالجداول الخوارزمية اللازمة للتشفير.

ومثلاً، أثّرت «وكالة الأمن القومي» في تبني خوارزمية توضع في الخلويات من النوع الثاني المعروف باسم «جي إس إم» (GSM)، كي تتمكن من اختراقها بسهولة⁽⁷³⁾.

وهناك مثل معروف بشكل واسع هو أن الوكالة زرعت «باباً خلفياً» في محرّك مهمّته توليد الأرقام العشوائية المتعلقة بعمليات تبادل البيانات والمعاملات بواسطة الإنترنت، ثم ضغطت كي يجري تبني ذلك المحرّك على نطاق واسع⁽⁷⁴⁾. وترمي تلك الجهود لتوهين التشفير الذي يستخدمه الجمهور لحماية الاتصالات بواسطة الإنترنت وعمليات البحث عن المعلومات في تلك الشبكة، لكنها جهود لم تكلّل بالنجاح.

في الفصل الخامس، تناولت ظهور «مجموعة عمليات الدخول المنسقة» (اسمها المختصر «تاو») التابعة لـ «وكالة الأمن القومي»، وهي مختصة في اختراق الإنترنت. وإضافة إلى عمليات الاختراق المباشر للحواسيب وأجهزة صنع الشبكات الرقمية، تنكّرت الوكالة على هيئة مواقع كـ «فيسبوك» و«لينكدن» (وربما مجموعة من المواقع الشبكية الأخرى)⁽⁷⁵⁾، لتخترق حواسيب معينة، ولتوجّه الحركة الإلكترونية في الموقعين (وربما مواقع أخرى) إلى مواقع مزيفة أنشأتها الوكالة بهدف التجسّس على الجمهور. وكذلك تستطيع «قيادة الاتصالات المركزية» في المملكة المتحدة أن تعثر على صورك الحميمة في «فيسبوك»، وترفع بشكل زائف أعداد زوّار موقع معين، وتعبث في تسجيلات الفيديو في موقع ما، وتمحو حسابات بأكملها من الإنترنت، وتسطو على استطلاعات الرأي وأكثر من ذلك بكثير⁽⁷⁶⁾.

وإضافة إلى انعدام الثقة العميق الذي تولّده تلك الممارسات في صفوف جمهور الإنترنت، فإنها تفرض على «وكالة الأمن القومي» ضمان أولوية الرقابة على حساب الأمن. وبدلاً من تحسين أمن الإنترنت لمصلحة الجميع، فإنّ ما تفعله الوكالة فعلياً هو ضمان بقاء الإنترنت غير آمنة؛ خدمة لمصالح الوكالة واستمرارية قدرتها على اختراق تلك الشبكة.

يتسبّب ذلك بالأذية لنا جميعاً؛ لأن الوكالة ليست الطرف الوحيد الذي يستفيد من زعزعة الأمن الشبكي. هناك حكومات وتنظيمات إجرامية تستفيد من ذلك أيضاً. وهناك عدد مدّهِش من تقنيات الاختراق على الإنترنت ليست حكرّاً على «وكالة الأمن

القومي»، وفق ما بيّنته وثائق سنودن، بل إنها ليست حكرًا على أجهزة الاستخبارات التابعة للدول أيضاً. إنها تقنيات اختراق برسم من يدفع بسخاء لشرائها⁽⁷⁷⁾. وناقش بعض الأكاديميين إمكان إعادة صنع تقنيات تستخدمها الوكالة لجمع البيانات وتحليلها، بواسطة نُظُم مفتوحة المصدر لوضعها بتصرف الجمهور مجاناً، وكذلك إتاحة تلك التقنيات للشركات التي تصنع النُظُم الرقمية التجارية أيضاً⁽⁷⁸⁾.

ومثلاً، عندما كنتُ أعمل في صحيفة الغارديان البريطانية، استماتت «وكالة الأمن القومي» كي تمنعنا من كشف برنامج معين كانت تعتبره فائق السرية، ويحمل اسم «كوانتوم» (Quantum)⁽⁷⁹⁾. ويتعلّق عمل البرنامج بتقنية اسمها «حقن الباكيث» (*) (Packet Injection)، وهي أساساً تقنية تتيح للوكالة اختراق الكمبيوتر⁽⁸⁰⁾. وبالنتيجة، تبين أن الوكالة لم تكن الطرف الوحيد الذي يستخدم تلك التقنية. إذ تستخدم الحكومة الصينية تقنية «حقن الباكيث» لمهاجمة الحواسيب⁽⁸¹⁾. وتبيع شركة «هاكنغ تيم»، المختصة بصنع أسلحة الفضاء الافتراضي، التقنية عينها لأي حكومة ترغب في الدفع بسخاء لشرائه⁽⁸²⁾.

كذلك تستخدم تلك التقنية منظمات إجرامية عدّة. وهناك أدوات تقنية لاختراق الكمبيوتر موضوعه بتصرّف الأفراد⁽⁸³⁾. كانت تلك الأشياء جميعها موجودة عندما كتبتُ عن تقنية «كوانتوم». وباستعمال معرفتها لمهاجمة الآخرين، بدلاً من بناء نظام دفاعي على الإنترنت، أدّت أعمال الوكالة إلى وضع تقنية «حقن الباكيث» في يد كل من يقدر على دفع ثمنها ليستعملها في اختراق الحواسيب.

وحتى عندما تبتكر تقنيات داخل «وكالة الأمن القومي»، فإنّها لا تبقى حكرًا على الوكالة لفترة طويلة⁽⁸⁴⁾. إذ إنّ البرامج السرية اليوم تصبح غداً موضوعاً لرسالة دكتوراه، ثم تتحوّل أداة في يد الـ «هاكرز» في اليوم التالي. وهناك مثل عمليّ

(*) تتحرّك البيانات على الإنترنت ضمن رزم محدّدة تشبه المقطورات في قطار طويل. وتسمى كل مجموعة (أو مقطورة) «باكيث»، وتتبع تسلسلاً رقمياً معيّناً، يربطها بالبقية، ما يضمن استمرارية حركة البيانات.

على ذلك: استعملت تقنيات عسكرية مخصصة للحرب الافتراضية في صنع فيروس «ستاكس نت»، وسرعان ما صارت أدوات في أيدي عصابات الجريمة المنظمة. وهناك برامج رقمية لكسر كلمات المرور باعتهها شركة «إلكومسوفت» (Elcomsoft) للحكومات، وسرعان ما استخدمت لاختراق السحابة المعلوماتية التابعة لشركة «آبل» والمسماة «آي كلاود» (iCloud) وسرقة صور المشاهير⁽⁸⁵⁾. وما كانت ذات مرة برامج سرية لمراقبة خلويات الأفراد، صارت الآن سلعة شائعة الاستعمال⁽⁸⁶⁾.

تأثر عمل الإنترنت كثيراً برغبة الحكومة الأمريكية في ممارسة رقابة غير مقيدة على تلك الشبكة. وعندما تضحى الرقابة عملاً تعاونياً بين حكومات عدة، تتفوق متطلبات ذلك الوضع على المعطيات الأخرى كافة. ويعتمد مهندسو الشبكات إلى تبني تصاميم تتجاوب مع حاجات الرقابة لدى الحكومات، وتستمر تلك التصاميم لعقود طويلة ببساطة؛ لأنه من الأسهل الاستمرار في عمل الأشياء عينها، بدل الإقدام على التغيير. وبإعطائها الأولوية للرقابة على حساب الأمن، ضمنت «وكالة الأمن القومي» أن نكون جميعاً غير آمنين.

أضرار جانبية من الهجمات السيبرانية

مع استمرار الاختراقات المتبادلة بين الأمم على الإنترنت، يصبح جمهورها جزءاً من أضرارها الجانبية باطّراد. في أغلب الأحيان، لا نعرف التفاصيل، لكن أحياناً تطفو على السطح بعض المعلومات عن مدى الضرر الذي يلحق بنا.

هنالك 3 أمثلة على ذلك. أولاً، استهدف الفيروس الإلكتروني «ستاكس نت» إيران⁽⁸⁷⁾، لكن حدث أن الفيروس تسرّب إلى ما يزيد على 50 ألف كومبيوتر في الهند وأندونيسيا وباكستان وغيرها، من بينها حواسيب تملكها شركة «شيفرون»⁽⁸⁸⁾ وشركات صناعية ألمانية⁽⁸⁹⁾، ولربما تسبّب أيضاً في سقوط قمر اصطناعي هندي في 2010⁽⁹⁰⁾. يزعم سنودن أن «وكالة الأمن القومي» تسببت خطأ في قطع الإنترنت عن سوريا في 2012⁽⁹¹⁾. وعلى نحو مشابه، يستخدم «سور النار العظيم» الرقمي

في الصين، تقنية تسمى «حَقْنِ نظام أسماء النطاق»^(*) (Domain Name System)، لمنع الوصول إلى مواقع معينة؛ وهي تقنية تؤدي إلى اضطراب في حركة الاتصالات بواسطة الإنترنت، حتى تلك التي لا تتصل بالصين ولا المواقع الممنوعة⁽⁹²⁾.

كلما زادت الاختراقات المتبادلة بواسطة الإنترنت بين الأمم، سواء لإحداث ضرر أم للحصول على معلومات استخباراتية، أضحت الشبكات الرقمية المدنية أكثر عرضة لأن تتحول إلى مجرد ضرر جانبي.

تضرر المصالح الوطنية

في الفصل 9، ناقشت الضرر الذي تلحقه نشاطات «وكالة الأمن القومي» باقتصاد الولايات المتحدة، إضافة إلى إلحاقها الضرر بالمصالح السياسية لأميركا.

وناقش عالم السياسة أيان برمر أن ما كشف للعموم عن نشاطات «وكالة الأمن القومي» أدى إلى «الإساءة بشدة إلى مصداقية الولايات المتحدة لدى كثيرين من حلفائها»⁽⁹³⁾. وعلى المسرح الدولي، تأذت مصالح الولايات المتحدة بعمق، إذ علمت دولة تلو الأخرى عن تلصص أميركا على قادتها⁽⁹⁴⁾. شمل ذلك بلداناً صديقة في أوروبا وآسيا وأميركا اللاتينية. وبصورة خاصة، تأذت العلاقات بين أميركا وألمانيا عندما كشفَ علانية أن «وكالة الأمن القومي» تجسست على هاتف المستشار الألمانية أنغيلا ميركل⁽⁹⁵⁾. وكذلك تجاهلت الرئيسة البرازيلية ديلما روسيف دعوة إلى عشاء عمل في الولايات المتحدة - وهي المرة الأولى لرئيس برازيلي - بسبب الغضب الذي شعرت به روسيف وبلاندا من رقابة الوكالة⁽⁹⁶⁾.

تحدث أشياء أكثر من ذلك كثيراً خلف الستار، وتمر بأقنية دبلوماسية شديدة الخصوصية. إذ لا مجال للتعامل برقة مع تخريب الولايات المتحدة علاقاتها وموقعها وقيادتها الدولية، بأثر من برنامجها الشرس في الرقابة.

(*) يعمل "نظام أسماء النطاق" على الربط بين الاسم الفعلي لصاحب الكمبيوتر، وهوية الحاسوب الإلكترونية المؤلفة من سلسلة أرقام تُعطى له عند الانتهاء من صناعه.

الجزء الثالث

كيف نتصرف بشأنها؟

12

المبادئ

تتعدّد الأضرار الناجمة عن الرقابة العامة، وتتجاوز كلفتها على الأفراد والمجتمع بأشواط ما تقدّمه من منافع. يجب على الجميع فعل شيء ما للسيطرة عليها، بل إنهم يقدرّون على ذلك. وقبل التقدّم باقتراحات محدّدة تقنياً وقانونياً واجتماعياً، أود أن أستهل الفصل ببعض المبادئ العامة. وتمثّل المبادئ حقائق شاملة عن الرقابة وكيفية التعامل معها، كما تنطبق على الحكومات والشركات معاً.

يشكّل جميع المبادئ الجزء السهل من الموضوع؛ فيما الأصعب هو تطبيقها في أوضاع محدّدة. «الحياة والحرية والبحث عن السعادة» هي مبادئ نُجمع عليها، لكن مجرد إلقاء نظرة على مسار الأمور في العاصمة واشنطن، تكفي لإظهار مدى صعوبة تطبيقها. حضرت نقاشات ومنتديات حوار كانت الأطراف المختلفة فيها متّفقة على المبادئ العامة بخصوص جمع البيانات والرقابة والإشراف والأمن والخصوصيّة، لكن ذلك لم يحل دون اختلافها بشدّة حول طرق تلك المبادئ في الواقع فعلياً.

الأمن والخصوصيّة

غالباً ما يوصف ذلك الضرب من النقاش بعبارة «الأمن مقابل الخصوصية». تملي علينا تلك الرؤية المبسّطة أن نجري نوعاً من المقايضة المبدئيّة بين الأمن، بمعنى أنه كي نكون آمنين يجب أن نُضحي بخصوصيّتنا ونستسلم للرقابة. وإذا

أردنا مستوى معيناً من الخصوصية، يجب أن نقرّ بضرورة التضحية بجزء من أمننا للحصول عليه.

إنها مبادلة زائفة. أولاً، يصح القول إن بعض إجراءات الأمن تتطلب من الناس تخلياً عن الخصوصية، لكن بعضها الآخر لا يمسّ الخصوصية كلياً؛ كأقفال الأبواب، السياجات المرتفعة، الحرس، الأبواب المحصنة لقمرة القيادة في الطائرة، وغيرها. وثانياً، من الناحية المبدئية، ثمة تحالف بين الخصوصية والأمن. عندما نفقد الخصوصية، نشعر بأننا مكشوفون وعرضة للخطر؛ نشعر بأمن أقل. وكذلك عندما تكون مساحاتك الشخصية وسجلاتك غير آمنة، تمتلك خصوصية أقل⁽¹⁾. يتحدث التعديل الأساسي الرابع في الدستور الأميركي عن «حق الناس في أن يكونوا آمنين في أشخاصهم وبيوتهم وأوراقهم وممتلكاتهم الشخصية المنقولة» (التشديد من المؤلف). وأقرّ واضعو الدستور بأن الخصوصية ركن أساسي في أمن الأفراد.

لذا، يؤدي صوغ النقاش على هيئة مبادلة بين الأمن والخصوصية إلى تقويات منحرفة. وفي أغلب الأحيان، تصاغ تلك المبادلة في صيغة الكلفة المالية: «كم تدفع من أجل الخصوصية؟» أو «كم تدفع للحصول على الأمن؟» لكن ذلك يمثل مبادلة زائفة أيضاً. إن تكاليف انعدام الأمن حقيقية وعميقة، حتى كفكرة مجردة. وكذلك فإن تكاليف انعدام الخصوصية واضحة وجلية كفكرة مجردة، وتغدو ملموسة بمجرد أن يفقدها المرء ويعاني تأثيرات غيابها. وللسبب عينه، لا نعطي للخصوصية مكانتها المستحقة عندما نمتلكها، ولا نفهم قيمتها فعلياً إلا عندما نفقدها. وللسبب عينه، نسمع من يقول إن الناس غير مستعدة لأن تدفع مقابل خصوصيتها، وإن الأمن يتفوق على الخصوصية بالمطلق.

عندما تُصاغ مبادلة الأمن بالخصوصية على شكل خيار بين الحياة [الأمن] والموت، ينتهي النقاش العقلاني كلياً⁽²⁾. كيف يمكن للمرء أن يتحدث عن الخصوصية عندما تكون حياة الناس على المحك؟ إذ يكون الناس المذعورون أشد

استعداداً للتضحية بخصوصيتهم مقابل الشعور بالأمن. ويفسر ذلك سبب إعطاء الحكومة الأميركية سلطة مطلقة في فرض رقابة عامة عقب هجمات الإرهاب في 9/11. إذ قالت الحكومة أساساً⁽³⁾ إنه يجب علينا جميعاً أن نتخلى عن خصوصيتنا مقابل الأمان؛ ولم تكن لغالبيتنا معرفة بخيار أفضل، ولذا قبلت بتلك المبادلة الفاوستية^(*).

تتمثل المشكلة في أن الوزن الكامل لانعدام الأمن يوضع في الكفة المقابلة للغزو التدريجي للخصوصية. تفعل محاكم أميركا ذلك، قائلة أشياء من نوع «نقر بأن هناك خسارة للخصوصية في برنامج حكومي أو آخر، لكن ثمن تفجير قنبلة ذرية في نيويورك، يفوق ذلك بكثير». إنه تمثيل ضبابي للمبادلة. وليست المسألة أن تفجيراً نووياً يغدو مستحيلاً إذا خضعنا للرقابة جميعاً، ولا أنه يصبح قدراً لا مفر منه إذا لم تحدث تلك الرقابة. الحال أن احتمال حدوث ذلك هو ضئيل فعلياً، ولا يؤدي غزو برنامج الأمن للخصوصية، إلى خفضه نظرياً إلا بقدر فائق الضآلة. إذاً، يجب إعادة النظر في المبادلة.

وعلى وجه العموم، يجب ألا يكون هدفنا هو البحث عن مبادلة مقبولة بين الأمن والخصوصية؛ لأنه من المستطاع [والواجب] الاحتفاظ بكليهما معاً سوياً⁽⁴⁾.

تقديم الأمن على الخصوصية

تتضارب متطلبات الأمن والخصوصية. ويصعب مراقبة نظام صُمم لغايات الأمن. وبالعكس، تصعب حماية نظام صُمم لتسهيل رقابته. وتسدد قدرات الرقابة المثبتة في نظام ما ضربة إلى أمنه؛ لأننا لا نعرف كيف نبني نظاماً لا يسمح بالرقابة إلا للأشخاص الموثوقين وحدهم. ونوقش ذلك في الفصل 11.

(*) إشارة إلى شخصية خيالية هو الشاب فاوست الذي عقد صفقة مفادها أن يحتفظ بشبابه ووسامته إلى الأبد، مقابل بيع روحه إلى الشيطان.

لنلاحظ أيضاً أنه بالنسبة للمجتمع ككل، يمتلك الأمن أهمية حاسمة أكثر من مسألة الرقابة. وبقول آخر، يجب علينا اختيار بنية تحتية للمعلومات تكون آمنة ومنيعة على الرقابة، بدلاً من بنية غير آمنة يسهل فرض رقابة عليها⁽⁵⁾.

تنطبق تلك الحاجة على وجه التعميم. إذ يسهل استخدام بنيتنا التحتية في المعلومات، لأغراض سيئة وجيدة. يقود سُراق البنوك سياراتهم على الطرق السريعة، يستخدمون الكهرباء، يشتررون أجهزةهم من المحلات الكبرى، ويتناولون وجباتهم في المطاعم التي تفتح على مدار الساعة، تماماً مثلما يفعل الناس الشرفاء. ويتشارك الأبرياء والمجرمون في استعمال الخليوي والبريد الإلكتروني والمخازن الشبكية من نوع «دروب بوكس» (Drop Box). ويهطل المطر على العادل والظالم معاً.

وعلى الرغم من ذلك، يستمر المجتمع في تدبر أموره لأن الاستخدامات الشريفة والإيجابية والمفيدة للبنية التحتية تفوق كثيراً الاستخدامات السلبية والمؤذية وغير الشريفة. لا يمثل سُراق البنوك سوى نسبة لا تذكر ممن يقودون سياراتهم على الطرقات السريعة، وكذلك الحال في نسبة المجرمين إلى إجمالي مستخدمي البريد الإلكتروني. ويبدو أكثر منطقية أن تبنى تلك النظم كلها كي تخدم غالبيتنا التي تحتاج إلى الأمن من المجرمين والمتسوقين الشبكيين الذين يسطون على حسابات الآخرين، بل من حكوماتنا أحياناً.

وعندما نضع نظاماً تراتبياً لأولويات الأمن، نستطيع حماية تدفق المعلومات عالمياً— بما فيه معلوماتنا وبياناتنا— من التنصت والهجمات الأكثر إيذاءً كالسرقة والتخريب. ويفتح المجال لحماية تدفقات معلوماتنا من الحكومات والمجرمين واللاعبين غير الرسميين. حينها، نجعل العالم أكثر أمناً ككل.

يعطي برنامج «تور» (Tor) مثلاً ممتازاً⁽⁶⁾. ويتميز «تور» بأنه يعمل بنظام المصدر المفتوح المجاني، ويمكنك أن تستخدمه من أجل الإبحار على الإنترنت من دون

كشف هويتك. جرى تطويره أصلاً بفضل تمويل من «مختبر البحوث» التابع للبحرّية الأميركية، ثم مولته وزارة الخارجية. ويستخدمه المنشقون في العالم أجمع للنجاة من الرقابة والحجب. وبديهي القول إنه يستعمل أيضاً من قِبل المجرمين للغاية نفسها. ويعمل صانعو «تور» على تطويره باستمرار كي يقدر على التملّص من محاولات الحكومة الصينية حظره على مواطنيها. ونعلم أيضاً أن «وكالة الأمن القومي» حاولت كسر شيفرته باستمرار⁽⁷⁾، لكنها فشلت⁽⁸⁾، على الأقل وصولاً إلى العام 2007 وفق ما بيّنته وثائق سنودن. ونعلم أن الـ «إف بي آي» استمرت في اختراق الحواسيب في 2013 و2014؛ لأنها فشلت في محاولة كسر شيفرة «تور»⁽⁹⁾. في الوقت نفسه، نعتقد بأن أشخاصاً عملوا المصلحة «وكالة الأمن القومي» و«القيادة الحكومية للاتصالات» البريطانية، يساعدون خفية في الحفاظ على شيفرة «تور» وأمنها⁽¹⁰⁾. ويصل بنا الكلام إلى مآزق: إما أن «تور» قوي بما فيه الكفاية فيحافظ على خفاء من نريد ومن لا نريد، أو أنه ضعيف فلا يحافظ على خفاء الطرفين كليهما. بديهي أنه لن يأتي زمن خلو من التجسّس. ويكون سذاجة الاعتقاد بعكس ذلك. فمنذ بداية التاريخ، تلجأ الحكومات إلى التجسّس⁽¹¹⁾، بل ترد قصص عن التجسّس في التوراة⁽¹²⁾. يبرز سؤال فعلي عن نوع العالم الذي نصبو إليه. هل نريد فعلياً تخفيف التفاوت في القوى بالحد من قدرات الحكومة على الرصد والحجب والتحكّم؟ أم إننا نسمح للحكومة بزيادة سلطتها علينا؟

«الأمن يتقدّم على الرقابة» ليس قانوناً ثابتاً بالطبع. هناك أوقات تقتضي تصميم نظام للحماية من تلك الأقلية غير الشريفة التي تعيش بيننا. ويعطي أمن الطائرات مثلاً على ذلك، إذ لا يمثل عدد الإرهابيين بالنسبة لإجمالي من يسافرون جواً سوى أقلية ضئيلة تماماً. وعلى الرغم من ذلك، تصمّم المطارات كلها حول فكرة الحماية من تلك الفئة الفائقة الصغر؛ لأن الفشل في الأمن على متن طائرة يؤدي إلى كوارث أكبر كثيراً من تفجيرات القنابل الإرهابية في أمكنة أخرى. في المقابل، لا نصمّم مجتمعتنا بأسره [ليس بعد] حول فكرة الحماية من الإرهاب⁽¹³⁾.

كذلك هنالك أوقات نحتاج فيها لوجود رقابة ملائمة في النُظم. إذ نرغب في أن تكون خدمات الشحن البحري قادرة على تتبّع الطرود في الوقت الحقيقي. نرغب أيضاً في أن يعرف من يرّدون أولاً على الاتصالات الطارئة، ومصدر تلك المكالمات. وبالطبع، لا نستعمل كلمة «رقابة» في تلك الأحوال، بل نلجأ إلى عبارات ملطّفة من نوع «تتبع الطرود».

في تلك الأحوال، يبرز مبدأ عام مفاده أن النُظم يجب أن تتبنى حدّاً أدنى من الرقابة يكون ضرورياً كي تستمر في العمل، إضافة إلى اكتفاء الرقابة حين تكون مطلوبة؛ بالحدّ الأدنى الضروري من المعلومات مع الاحتفاظ بها أقصر وقت ممكن.

الشفافية

الشفافية أمر ضروري لكل مجتمع حرّ ومنفتح. تتيح القوانين الحكومية المفتوحة وقوانين حرية المعلومات للمواطنين معرفة ما تفعله الحكومة، كما تمكّنهم من إنجاز واجبهم الديمقراطي في الإشراف على نشاطاتها. وفي القطاع الخاص، تؤدي قوانين الصراحة في الشركات وظيفته مماثلة. بالطبع، تحتاج الحكومة والشركات معاً إلى شيء من السريّة، ولكن كلّما ازدادوا شفافية، استطعنا أن نقرّر عن معرفة مدى ثقتنا بهم⁽¹⁴⁾. وحتى الآن، تملك الولايات المتحدة حكومة منفتحة تماماً مع قوانين لحرية المعلومات، لكن هناك معلومات كثيرة لا ينطبق عليها ذلك⁽¹⁵⁾.

بالنسبة للمعلومات الشخصية، تكون الشفافية مباشرة إلى حدّ كبير: إذ يملك الناس الحق في معرفة المعلومات والبيانات التي جُمعت عنهم، كم ذهب منها إلى الأرشيف، كيف استُخدمت، ومن قبل مَنْ. نكون ميّالين لارتياح إلى الرقابة بأنواعها، إذا أحطنا علماً بتلك الأشياء. يفترض بسياسات الرقابة أن تعطي الناس تلك المعلومات، بدل تعمّد إدخالها في ضبابيّة تُفقد القدرة على إنارة الأمور.

نحتاج أيضاً إلى معرفة الخوارزميات المؤتمتة التي يناط بها التوصل إلى أحكام وخلاصات بشأننا استناداً إلى بياناتنا، إما بنشر شيفرة الخوارزميات أو بشرح وافٍ عن طريقة عملها. وحاضراً، لا نستطيع الحكم على مدى عدالة الخوارزميات التي تستخدمها «أمن إدارة النقل» في إعداد قوائم من يجب إخضاعهم لـ «تفتيش مسحي خاص»⁽¹⁶⁾. وينطبق الأمر على الخوارزميات التي تستخدمها «مصلحة المداخل الداخلية» لانتقاء من يجب التدقيق في مداخلهم⁽¹⁷⁾. وتكرّر الحال عينها بالنسبة للخوارزميات التي يستخدمها محرك البحث للبتّ في شأن الصفحات التي يمكننا مشاهدتها على الإنترنت؛ وخوارزميات التوقع الشرطي التي تحدّد من يجدر جلبه للتحقيق وما هي الأحياء التي يجب استهدافها من قبل دوريات الشرطة؛ وخوارزميات الوضع الاتهامي التي تقرّر جدارة الأفراد في الحصول على رهونات عقارية. هناك شيء من السرية يفرض نفسه في تلك الأمور، لمنع الناس من التلاعب بالنظام، لكن الإكثار من السرية ليس ضرورياً البتّة. ويتيح «قانون حماية المعلومات» في «الاتحاد الأوروبي»، الكشف عن جلّ تلك المعلومات.

أبدو كمن يتناقض مع نفسه. من ناحية، أناصر الخصوصية الفردية على حساب الرقابة المفروضة. ومن الناحية الثانية، أؤيد تقديم شفافية الحكومة والشركات على حساب السرية المؤسسية. ويكمن السبب في تأييدي الأمرين معاً، في الخلل حاضر في ميزان القوة بين الناس والمؤسسات⁽¹⁸⁾. إذ تفوق قوة المؤسسات ما يملكه الجمهور، ويتنامى الخلل باستمرار. وتعمل سرية المؤسسات على زيادة قوتها، ما يزيد الخلل أيضاً. ويحمل الأمر تهديداً أساسياً للحرية الشخصية. كذلك تنمي الخصوصية الفردية قوة الأفراد، ما يخفف الخلل؛ وهو أمر مفيد للحرية. وينطبق الأمر تماماً على الشفافية والرقابة⁽¹⁹⁾. إذ تخفض الشفافية المؤسسية الخلل في القوة، وهو أمر إيجابي⁽²⁰⁾. وتزيد رقابة المؤسسات على الأفراد من الخلل، وهو أمر سيئ تماماً.

لا تأتي الشفافية بسهولة⁽²¹⁾. ولا يرغب القوي في التدقيق به. ومثلاً، تبدي الشرطة نفوراً متزايداً من تقييمه. في الولايات المتحدة بأكملها، تلاحق الشرطة وتضايق من يسجلون أشرطة عنها⁽²²⁾، بل إن سلطات قضائية عدت تلك الأشرطة غير قانونية⁽²³⁾. ويعتمد رجال الشرطة في شيكاغو تسمية الكاميرات، ما يظهر كأنه مسعى لإخفاء أفعالهم بالذات⁽²⁴⁾. وترفض دائرة الشرطة في «سان دييغو» كل طلبات الحصول على أشرطةها، مصرّة على أنها جزء من تحقيقات جارية⁽²⁵⁾. وخلال التظاهرات الاحتجاجية للعام 2014 في بلدة «فيرغسون» بولاية «ميسوري»، التي اندلعت إثر مقتل رجل أسود غير مسلح على يد الشرطة، حرصت الشرطة باستمرار على منع المحتجين من تصويرها، واعتُقل مراسلون كُثُر بسبب توثيق تلك الحوادث⁽²⁶⁾. وذهبت الشرطة في «لوس أنجلوس» إلى حدّ تخريب التسجيلات الصوتية في سيارات دورياتهم، على الرغم من أن القانون يتطلب وجودها.

وبصورة دائمة، تقاوم الحكومات والشركات قوانين الشفافية من الأنواع كافة. في المقابل، يتعرض عالم السرية للتبدّل. وكتب الباحث في قانون الخصوصية بيتر سواير عن التناقض المستمر في دورة حياة الأسرار⁽²⁷⁾. ولاحظ أن الأسرار عموماً صارت تنكشف أسرع من العادة. وتجعل التكنولوجيا الأسرار أصعب حفظاً، وتضعب طبيعة الإنترنت الاحتفاظ بها لزمّن طويل. يكفي الضغط على زر «أرسل» إلى نشر غيغابايتات من المعلومات، بمثل لمح البصر. وفي كل سنة، تزيد قدرة مفاتيح الذاكرة الخارجية على تخزين المعلومات. وتحتاج الحكومات والشركات إلى افتراض أن أسرارها صارت أشدّ عرضة للانكشاف، وبسرعة كبيرة، أكثر من أي وقت مضى.

يترتب على تقاصر دورة حياة الأسرار نتائج منها أن انكشافها صار أكثر إيذاءً. أشارت إحدى وثائق سنودن إلى تجسّس «وكالة الأمن القومي» على هاتف المستشارة الألمانية أنغيلا ميركل⁽²⁸⁾. لم تحمل الوثيقة تاريخاً محدداً، لكنها ترجع بوضوح إلى سنوات قليلة خلت. لو كُشِفَت الوثيقة عينها بعد عشرين سنة من الآن، لكانت ردة

الفعل عليها في ألمانيا مختلفة جداً عن الزجيرة العامة التي عكّت في 2013، فيما ميركل لا تزال في مكتب المستشارية وتعلّق الأمر بحدث جارٍ، وليس حدثاً من التاريخ.

تصعّب التغيّرات الثقافية الجارية حاضراً الحفاظ على الأسرار. في الأيام الخوالي، كان الحفاظ على أسرار المؤسسة جزءاً من ثقافة تستمر مدى الحياة. وكانت الاستخبارات توظّف أشخاصاً في مقتبل العمر، وتسند إليهم وظائف تستمر طيلة حياتهم. كانت أشبه بنادٍ خاص يحتكره الرجال، ومملوء بالكلمات المشفرة والمعرفة السريّة⁽²⁹⁾. وكذلك كان عالم الشركات مكتظاً بمن يعملون مدى الحياة. خلت تلك الأيام. هناك وظائف كثيرة في عالم الاستخبارات يجري تعهدها إلى أطراف تعمل خارجه، ولم يعد مفهوم «وظيفة مدى الحياة» موجوداً في عالم الشركات. صارت قوى العمل مطوعة، والوظائف قابلة للتعهيد، والأشخاص قابلين للاستبدال. بات العُرف السائد هو الانتقال من رب عمل إلى آخر⁽³⁰⁾. ويعني ذلك أن الأسرار يجري تشاركها بين عدد أكبر من الناس الذين يتدنى اهتمامهم بالحفاظ عليها. لتذكّر أن خمسة ملايين شخص في الولايات المتحدة يحملون أذونات أمّية، وأن معظمهم متعاقدون وليسوا موظفين حكوميين⁽³¹⁾.

هناك إيمان متصاعد بقيمة الانفتاح، خصوصاً في أوساط الشباب. ويبدى الأصغر سنّاً ارتياحاً أكبر للتشارك في المعلومات الشخصية، بالمقارنة مع من هم أكبر سنّاً⁽³²⁾. إذ يؤمن الشباب أن المعلومات يجب أن تكون حرة، والأمن يأتي من انتشار المعرفة بين العموم، إضافة إلى النقاشات بينهم. يعبر الشباب عن أشياء شخصية على الإنترنت، كما نشروا بأنفسهم صوراً محرّجة لهم على مواقع شبكات التواصل الاجتماعي. وهجرهم من يحبونهم علانية في المنتديات الشبكية. تشارك الشباب بأشد الطرق إرهاباً، لكنهم اجتازوا ذلك بسلام. من الصعوبة بمكان الترويج في صفوف ذلك الحشد الشبابي، أن حق الحكومة في السريّة يتقدّم على حق الناس في المعرفة⁽³³⁾.

إنها ميول تكنولوجية واجتماعية جيدة. يجب النضال من أجل الشفافية، كلما أمكن ذلك⁽³⁴⁾.

الإشراف والموثوقية

من أجل استمرارية معظم المجتمعات، يجب على الناس أن يعطوا الآخرين سلطة عليهم. يتضمن التنازل عن السلطة شيئاً من الخطورة بشكل لا مفر منه، وعلى مدار آلاف السنوات، طور البشر أطراً لحماية أنفسهم من تنازلهم عن السلطة لفئة منهم، وهي تشمل الشفافية والإشراف والموثوقية. إذا عرفنا كيف يستخدم الآخرون السلطة التي منحناها لهم بأنفسنا، نستطيع أن نضمن لأنفسنا أنهم لن يسيئوا استخدامها؛ وإذا قدرنا أن نعاقبهم عندما يسيئون، نستطيع أن نثق بهم أكثر عندما نعطيهم السلطة. يمثل ذلك عقداً أساسياً في الديمقراطية.

هناك مستويان من الإشراف. هناك أولاً الإشراف الاستراتيجي الذي يلخصه السؤال عن مدى صحة القوانين التي نتبناها. ومثلاً، تستطيع «وكالة الأمن القومي» تنفيذ إجراءاتها الخاصة كي تتأكد من اتباعها القانون، لكن يجب ألا تقرر القوانين التي يجب عليها اتباعها. شُرح ذلك بطريقة حسنة تماماً من قبل مايكل هايدن، المدير السابق لـ «وكالة الأمن القومي»: «أعطني حدود الصندوق الذي تسمح لي بالعمل ضمنه، وسوف ألعب حتى الحدود القصوى للصندوق... أنتم، الشعب الأمريكي، أعطوني بواسطة ممثليكم المنتخبين حقلاً للعب، وسوف ألعب بكل قسوة فيه»⁽³⁵⁾. هناك معنى واحد تصح فيه هذه الأقوال: ليست وظيفته أن يسن القوانين، لكنه مخطئ في كل معنى آخر، وهو ما سأشرحه في الفصل 13.

في الحالين، يجب أن نتحسن في شأن الإشراف الاستراتيجي. نحتاج إلى نقاشات أكثر انفتاحاً عن الحدود التي ينبغي رسمها للحكومة ورقابتها. نحتاج إلى مشرعين مقتدرين في الإشراف، وتطوير ردود بعيدة النظر. كذلك نحتاج إلى محاكم منفتحة ومستقلة تدعم القوانين ولا تصادق تلقائياً على ممارسات الوكالة، وتقارير دورية

عن أعمال الحكومة، وصحافة رأي عام نابضة، ومجموعات متابعة لتحليل أفعال المسكين بالسلطة وفتح جدال معهم، إضافة إلى إطار تشريعي يستبق الأمور ويحذر من المخاطر. وكذلك نحتاج جمهوراً مهتماً. وسوف أتحدث عن تلك الأمور في الفصل 13 أيضاً.

وهناك المستوى الثاني من الإشراف، وهو تكتيكي يلخصه السؤال عن مدى الالتزام بالقوانين. وتتضمن آلياته الإجراءات والتدقيقات والموافقات وبروتوكولات التصدي للمشاكل وغيرها. مثلاً، درّبت «وكالة الأمن القومي» محلّليها على القوانين التي تتحكّم بعملها، ونُظِم التدقيقات التي مهمّتها التأكد من الالتزام فعلياً بالقوانين، كما أرسّت إجراءات في الإبلاغ وعقوبات تصحيحية في حال عدم الالتزام.

تمارس المنظمات المختلفة إشرافاً تكتيكياً متبادلاً على بعضها بعضاً. وتعطي آلية الضمان مثلاً عن ذلك. من المؤكّد أننا نستطيع أن نثق بقوّات الشرطة عندما تنهض بعمليات التفتيش الواجبة عليها، ولكننا بدلاً من ذلك نطلب منها إبراز طلب التفتيش أمام طرف محايد - القاضي - الذي يضمن أنها أتبعّت القوانين قبل حصولها على أمرٍ من المحكمة بالتفتيش.

إن مفتاح الإشراف المتمكن هو الاستقلالية. ولذلك السبب، نبدي تشكّكاً دائماً بالتحقيقات الداخلية، حتى لو أجراها محام متحمّس. كانت تلك القضية الرئيسة مع المسؤول الأول عن الخصوصية في «وزارة الأمن القومي». أذكّر بوضوح ماري إلين كالاهاان التي شغلت تلك الوظيفة بين عامي 2009 و2012. كانت مؤيدة كبيرة للخصوصية، وأوصت بشطب برامج عدّة، بسبب ما أخذ تتعلق بالخصوصية. في المقابل، كانت تعمل تحت إدارة الوزيرة جانيت نابوليتانو، ما جعل عمل كالاهاان مقتصرأ على الاقتراحات. لو عملت كالاهاان خارج الوزارة، لامتلكت صلاحيات

تشريعية أوسع. ينجز الإشراف التكتيكي بشكل أفضل على يد هيئات تقييم خارجية تتمتع بمعرفة واسعة وتملك ما يكفي من طواقم العمل.

يمكن التفكير بالفارق بين الإشراف التكتيكي والاستراتيجي باعتباره موازياً للفارق بين عمل الأشياء بطريقة صحيحة، والقيام بالشيء الصحيح. ونحن بحاجة لكلا الأمرين معاً.

لا يسير أي من الأمرين بفعالية من دون الموثوقية. من توكل إليهم السلطة ليسوا بمنأى عن إساءة استعمالها مع النجاة من العقاب؛ يجب أن توضع عقوبات لإساءة استخدام السلطة. يساوي الإشراف من دون موثوقية عدم تغيير أي شيء، وفق ما تعلمنا التجربة مراراً وتكراراً. ووفق ما بين نسيم طالب، وهو مختص بتحليل المخاطر، يتدنى سوء استخدام المنظمات لسلطاتها عندما يحسّ الناس أن مصيرهم معلق بها⁽³⁶⁾.

تسهل المناداة بـ «الشفافية والإشراف والموثوقية»، لكن يصعب وضع هذه المبادئ موضع التطبيق فعلياً. وعلى الرغم من ذلك، يجب أن نحاول، وسأبين في الفصل القادم كيف نفعل ذلك. تعطينا هذه الأشياء الثلاثة ثقة بالنفس تجعلنا نثق بالمؤسّسات القويّة. إذا كنا سنسلس القياد لهم، فيجب طمأنتنا بأنهم سيعملون لمصلحتنا، ولا يسيئون استخدام تلك السلطة.

التصميم المرن

يعدّ وضع تصميم للمرونة مبدأً أساسياً، بل شبه فلسفي، في هندسة النظم. غالباً ما يفترض بالحلول التكنولوجية أن تكون كاملة. لكن، كما نعرف جميعاً، الكمال أمر مستحيل، وفي صلب بنية الناس والمنظمات والنظم أنها ليست تامة الكمال، بل فيها شيء من الخطل. وتعاني المنظمات كلها وجود اختلالات فيها، بداية من الوكالات الحكومية وصولاً إلى الشركات المتعددة الجنسيات.

لا تنجم الاختلالات من لاعيين سيئين داخل نُظُم من شأنها أن تكون كاملة لولا هم. تأتي الاختلالات من أشياء الدنيا العادية، والكادر المتوسط، والميل البيروقراطي. تعتبر ظاهرة «زحف المهمة»^(*) أحد أشكال الاختلال.

يأتي شكل آخر للخلل من أشخاص داخل المنظّمات يركّزون على الحاجات الضيقة للمنظمة، بدل التفكير في الإملاءات الواسعة لأفعالهم.

وتأتي الاختلالات أيضاً من التغيير الاجتماعي على غرار التغيير في قيمنا مع مرور الزمن. ويضيف التقدّم التكنولوجي اهتزازات جديدة إلى تلك الموجودة في النظام، ما يخلّ بالاستقرار⁽³⁷⁾.

إذا كانت الاختلالات المنهجية أمراً لا مفر منه، فعلياً تقبلها في القوانين والشركات والأفراد والمجتمع والمؤسسات الحكومية⁽³⁸⁾. يجب علينا تصميم نُظُم تتوقع الاختلالات، وتستطيع العمل على الرغم من وجودها. إذا وجب فشل شيء ما أو خرابه، فالأفضل أن يحصل ذلك بطريقة متوقعة. تلك هي المرونة⁽³⁹⁾.

في تصميم النُظُم، تتأتى المرونة من اجتماع عناصر تشمل تحمّل الخطأ، والتخفيف، والتأقلم، والوفرة، والتعافي، والتمسك بالبقاء⁽⁴⁰⁾. نحتاج تلك الأشياء في المشهديات المعقّدة والمتغيرة للتهديدات، وفق ما وصفته في الكتاب.

أدافع عن ألوان متنوعة من المرونة في نُظُمنا للرقابة ونُظُمنا التي تتحكّم في الرقابة أيضاً⁽⁴¹⁾. ويشمل ذلك المرونة حيال فشل البرامج والمكونات الإلكترونية، والمرونة حيال الاكتشاف التكنولوجي، والمرونة حيال التغيير السياسي، والمرونة حيال الضغط والإكراه. أدافع عن تصميم للأمن يعطي المرونة حيال الأهواء السياسية المتغيرة التي يحتمل أن تشرعن الرقابة السياسية. يمنح تداخل السلطات وتعدّدها مرونة حيال الضغوط الإكراهية. تقدّم القوانين المتقنة الصياغة مرونة حيال القدرات التكنولوجية المتبدّلة. بديهي القول أيضاً إنه من المستحيل الوصول

(*) انظر الفصل السابع.

إلى المرونة الكاملة في تلك الأمور، وناقلًا القول باستحالة المرونة الكاملة حيالها كلها. على الرغم من ذلك، يجب علينا بذل أفضل ما نستطيع، وصولاً إلى نقطة افتراض الاختلالات في مرونتنا.

عالم واحد، وشبكة واحدة، وحل واحد

هناك نقاشات كثيرة في الولايات المتحدة حول سلطة «وكالة الأمن القومي»، وأنّ لجمها يعطي قوّة للآخرين. إنّ نقاش مغلوط. لسنا أمام خيار بأن روسيا والصين وإسرائيل ستوقف عن التجسس، إذا توقفت الوكالة عنه. فعلياً، يجب علينا حسم الخيار بشأن بناء بنية معلوماتية تحتية تكون هشة أمام مهاجميها جميعاً، أو تكون مأمونة لمستخدميها كلهم.

منذ تأسيسها في 1952، مُخِضَت «وكالة الأمن القومي» الثقة لتنفيذ مهمّات لها طبيعة مزدوجة⁽⁴²⁾. في خطوة أولى، انخرطت «سيغنت» في اعتراض نُظُم الاتصالات لدى أعداء أميركا. وبعدها، تولى قسم «أمن الاتصالات»، «كومسك» (COMSEC)، حماية الاتصالات العسكرية الأميركية وبعض الاتصالات الحكومية من احتمال اعتراضها من قِبَل أعداء. وبدا منطقياً الجمع بين المهمتين؛ لأن معرفة آليات التنصّت ضرورية للحماية من التنصّت.

كانت المهمتان متكاملتين؛ لأن البلدان المختلفة استخدمت نُظُمًا مختلفة في الاتصالات، وكذلك استخدم المدنيون والطواقم البشرية العسكرية نُظُمًا مختلفة أيضاً. ووفق ما وصفته في الفصل 5، لم يعد ذلك العالم موجوداً. وحاضراً، باتت مهمّتا «وكالة الأمن القومي» متضاربتين.

ربما يحدّد القانون الطُرُق المشروعة للرقابة، لكن التكنولوجيا هي التي تقرّر مدى الرقابة وإمكاناتها. عندما نقرّر تقنيات الاتصالات التي يجب أن نبتّها، لا نستطيع أن ننظر إلى بلدنا [الولايات المتحدة] وحده. يجب أن ننظر إلى العالم بأسره.

لا نستطيع أن نوهن شبكات الأعداء، وإبقاء شبكاتنا محمية وآمنة في الوقت نفسه. وإذا تستغل أجهزة الاستخبارات عالمياً الثغرات في النظم الإلكترونية كي تتجسس على بعضها بعضاً، تستخدم عصابات الإجرام الثغرات نفسها كي تسطو على كلمات المرور التي تستعملها في حساباتك المصرفية؛ لأننا نستعمل جميعنا المنتجات والتقنيات والبروتوكولات والمعايير ذاتها؛ يكون لازماً علينا الخيار بين إعطاء كل شخص القدرة للتجسس على الآخر أو نجعل التجسس أمراً صعباً على الجميع. إنها الحرية في مواجهة التسلط، فإما أن ننجو جميعاً أو نهوي كلنا. كتب البروفسور جاك غولد سميث، وهو أستاذ قانون في جامعة هارفرد شغل منصب المدعي العام أثناء حكم الرئيس جورج دبليو بوش: «كل سلاح هجومي هو (احتمالاً) جزء من نظامنا الدفاعي، والعكس بالعكس»⁽⁴³⁾.

ومثلاً، يفرض «قانون مساعدة الاتصالات في تطبيق القوانين» أن تسمح الدارات الإلكترونية في الهواتف، بتنصت [حكومي] على المكالمات. ربما نتسامح مع ذلك بالنسبة لقوى الشرطة الأميركية؛ لأننا نثق عموماً بالإجراءات القضائية اللازمة للسماح للشرطة بالتنصت، ونميل للافتراض بأن الشرطة لن تسيء استخدام صلاحياتها. في المقابل، تُباع تلك الدارات نفسها عالمياً - أذكر بقصة التجسس على خلوي في اليونان، التي وردت في الفصل 11 - مع امتلاكها للقدرة على إتاحة التنصت. إذًا، يعود الخيار لنا: إما أن يكون الكل قادراً على التنصت، أو ألا يفعل أحد ذلك.

نطبق الوصف نفسه على الأداة الإلكترونية المسماة «آي أم أس آي - كاتشر»^(*) التي تتولى اعتراض المكالمات الخلوية وال «ميتا- داتا» المتصلة بها. ربما كانت أداة «ستنغراي» الشبيهة بـ «آي أم أس آي - كاتشر» سلاحاً سرّياً لدى ال «إف بي آي»، لكنها تقنية لم تعد سرّية أبداً⁽⁴⁴⁾. هناك عشرات من تلك الأدوات منشورة

(*) هي أساساً برج مزيف للاتصالات الخلوية. راجع الفصل 5

حول العاصمة واشنطن، لكن بقية البلاد تدار من قِبَل ما لا يُعلم من المنظّمات أو الوكالات الحكومية⁽⁴⁵⁾. وباطّراد، تدنو لحظة استخدامها إجرامياً. ولأننا عملنا على أن تكون شبكات الاتصالات الهاتفية قابلة للاختراق من قِبَل تلك الأدوات كي تساعد التحقيقات في الجرائم، فإننا أتحنا بالضرورة أن نستخدم ضدنا من المجرمين والحكومات الأجنبية.

في الفصل 11، أعطيت أمثلة جمة عن ذلك الأمر. وعموماً، يجب علينا أن نقرّر بشأن البنية التحتية للاتصالات التي نصبو إلى إنشائها: هل تكون مكرّسة للأمن والرقابة والخصوصية والمرونة أو لا؟ وعندها يستطيع كل شخص استخدام تلك البنية التحتية.

13

حلول للحكومة

في سياق كشوفات سنودن عن رقابة «وكالة الأمن القومي»، تبيّن أن الاقتراحات بشأن طُرُق إصلاح الاستخبارات القوميّة كانت غزيرة. في العام 2013، ألّف الرئيس باراك أوباما لجنة للمراجعة بشأن الرقابة والاستخبارات القوميّة، وتوصّلت تلك اللجنة إلى 46 توصية بصدد «وكالة الأمن القومي»⁽¹⁾. في العام 2014، وقّعت 500 منظمة وخبير ومسؤول من أرجاء العالم كافة، كنّت واحداً منهم، وثيقة «مبادئ دولية عن تطبيق حقوق الإنسان في رقابة الاتّصالات» (International Principles on the Application of Human Rights on Communications Surveillance) التي يُشار إليها غالباً باسم «المبادئ الضروري والنسبية» (Necessary & Proportionate Principles)⁽²⁾. وناقش الكونغرس وثائق عدّة تتضمّن إصلاحات صغيرة، ربما أقرّ بعضها عند ظهور الكتاب.

في هذا الفصل، أناقش الأمن القومي وإنفاذ القانون، وأقدّم توصيات عامة، بأكثر من كونها توصيفات تشريعيّة دقيقة، عن السياسة التي يجب اتّباعها في الأمرين كليهما. من السهل تنفيذ بعض التوصيات، لكن الأخرى تقترب من كونها أمّيات. وتعبّر كلها عن الطريق الذي أعتقد بأنّه يجب على الحكومة سلوكه.

لا أحاجج لمصلحة حرمان الحكومة كليّاً من الرقابة أو التجسّس. نحن فعليّاً منحنا صنّاع السياسة منذ زمن، ما يكفي من القوى لغزو خصوصيّة المواطن

والنفاذ إلى بياناتهم ومعلوماتهم. فعلنا ذلك عن معرفة مسبقة - وبارادة منا أيضاً - لأن ذلك يساعد في كشف الجرائم، ما من شأنه أن يجعلنا أكثر أماناً. يكمن الهدف فعلياً في التوصل إلى توازن بين حيازة المؤسسات الحكومية تلك القوى من جهة، وضمان عدم إساءة استخدامها من الجهة الأخرى. إذ نحتاج إلى الأمن الذي تؤمنه الحكومة، كما نحتاج إلى أن نكون آمنين من الحكومة نفسها. ونحاول التوصل إلى ذلك التوازن، وثائق كـ «دستور الولايات المتحدة» و«شرعة الاتحاد الأوروبي»، وإجراءات كالحصول على إذن قضائي للتفتيش. واختل ذلك التوازن في سياق سعينا المجنون إلى الأمن ضد الإرهابيين عقب هجمات 9 / 11.

"مبادئ عالمية عن تطبيق حقوق الإنسان في رقابة الاتصالات - ملخص 2014" (3)

شرعية: يجب صوغ حدود الحق في الخصوصية بوضوح ودقة في القوانين، ويجب مراجعتها بانتظام للتثبت من التناسب بين حمايات الخصوصية وسرعة التغيرات التكنولوجية.

هدف قانوني: يجب ألا يسمح بالرقابة على الاتصالات سوى في سياق السعي إلى تحقيق الأهداف المهمة للدولة.

ضرورة: يقع على الدولة واجب إثبات أن نشاطاتها في رقابة الاتصالات ضرورية لتحقيق هدف قانوني.

ملائمة: يجب أن تكون آلية رقابة الاتصالات فعالة في تحقيق هدفها القانوني.

تناسب: يجب أن ينظر إلى رقابة الاتصالات كعمل تدخل من أعلى مستوى، ويتدخل في حقوق الخصوصية وحرية الرأي والتعبير، إضافة لكونه يهدد أسس المجتمع الديمقراطي. وعلى نحو نموذجي، تتطلب الرقابة المناسبة في الاتصالات تحويلاً مسبقاً من مكوّن في السلطة التشريعية.

مُكوّن السلطة التشريعيّة: التحديد بشأن رقابة الاتّصالات يجب أن يكون من قِبَل مُكوّن في السلطة التشريعيّة يتمتع بالاستقلاليّة وعدم الانحياز.

إجراء مناسب: يتطلّب الإجراء المناسب إخضاع التدخل في حقوق الإنسان إلى إجراءات قانونيّة تكون متاحة للعموم، وأن تطبق بسواسيّة ضمن لجنة استماع عادلة وعلنيّة.

تنبيه المستخدم: يجب تنبيه الأفراد بشأن قرار فرض رقابة على اتّصالاتهم. في ما عدا حالاً وجد فيها مُكوّن السلطة التشريعيّة أن التنبيه يؤذي التحقيق، ويجب أن يعطى الأفراد فرصة لتحدي فرض الرقابة قبل حدوثها.

الشفافية: يقع على الحكومة واجب إتاحة معلومات كافية وعلنيّة، ما يمكن الجمهور العام من فهم طبيعة نشاطاتها الرقابية وأمديتها. وعموماً، يجب على الحكومة عدم منع مقدّمي الخدمات من نشر تفاصيل عن طبيعة ومدى تعاملاتهم الخاصة مع الحكومة في ما يتّصل بالرقابة.

إشراف الجمهور: يجب على الحكومات إرساء آليات مستقلة للإشراف بما يضمن شفافية رقابة الاتّصالات وموثوقيتها. يجب أن تمتلك آليات الإشراف سلطة الوصول إلى المعلومات كافة التي يحتمل أن تكون ذات دلالة بالنسبة لأفعال الحكومة.

نزاهة الاتّصالات والنُظم: يجب ألا يُرغم مقدّمو الخدمات والشركات البائعة للبرامج والمكوّنات الصلبة، على وضع قدرات رقابية أو «أبواب خلفية» في نُظُمهم؛ أو جمع أو الاحتفاظ بمعلومات معيّنة لمجرد خدمة أهداف رقابة الدولة.

ضوابط التعاون الدولي: وفقاً للحال، ربما تسعى الحكومات إلى الحصول على مساعدة من مقدّم خدمة أجنبي، بهدف ممارسة رقابة. يجب أن يضبط ذلك باتفاقيات واضحة وعلنيّة تضمن تطبيق أعلى مستوى في حماية الخصوصية، يكون قابلاً للاعتماد عليه في الأحوال كلها.

ضوابط ضد الوصول غير المشروع: يجب فرض جزاءات مدنيّة وجرميّة على كل طرف تثبت مسؤوليته عن ممارسة رقابة إلكترونيّة غير شرعيّة؛ ومن تطالهم تلك الرقابة لهم الحق في الوصول إلى آليات قانونيّة تضمن تعويضهم بشكل فعال. كذلك يجب تقديم حماية قويّة لمطلق صافرات الإنذار الذين يكشفون نشاطات رقابيّة مهددة لحقوق الإنسان.

أنا أتحّدث أساساً عن الولايات المتّحدة، على الرغم من أن التوصيات الواردة في هذا الفصل تصلح في أمكنة أخرى. في الولايات المتّحدة، يستطيع الرئيس تنفيذ بعض تلك التوصيات استناداً إلى السلطة التنفيذية بشكل أحادي، وبعضها يتطلّب موافقة الكونغرس، لكن بعضاً آخر يحتاج إلى سنّ تشريعات جديدة. وتملك بلدان أخرى قوانين خاصة بها عن الفصل بين السلطات. وبالطبع، ثمة بلدان يتطلّب فيها تنفيذ تلك التوصيات إحداث تغيير جذري في الحكومة.

سريّة أقل، شفافيّة أكثر

منذ 11/9، زعمت إدارتا بوش وأوباما تكراراً أن مستويات السريّة العالية أمر ضروري لمنع العدو من معرفة ما نفعله⁽⁴⁾. هناك مستويات من السريّة مورست في الحرب العالميّة الأولى، وما زال بعض منطقتها صالحاً. تملك الحقائق التكتيكيّة قيمة كبرى لمُدّة معيّنة، ومن المهم الاحتفاظ بها سرّاً طيلة تلك المدّة. وأحياناً، تبرز الحاجة للاحتفاظ بأسرار كبرى: كالمفاوضات مع البلدان الأخرى، هويّات العملاء الأجانب، الخطط العسكريّة وبعض مناحي الاستخبارات القوميّة⁽⁵⁾. وفي عودة إلى الفارق المهم بين التجسّس والرقابة، تتطلّب نظمتنا في التجسّس سريّة أعلى كثيراً مما تفعله نظيرتها في الرقابة.

في المقابل، نستطيع أن نكون أكثر شفافيّة في نواح عدّة. قارن السريّة الكثيفة التي تحيط بعمل «وكالة الأمن القومي» مع نطاق مُشابه نحز فيه نجاحات بصورة روتينيّة من دون رقابة مكثّفة: الشرطة ومكافحة الجريمة. ينظّم التعديل الرابع في

الدستور الأميركي قدرة الشرطة على ممارسة الرقابة، كما أن الأحكام القضائية بشأنها علنية. يستطيع المجرمون قراءة تلك الأشياء كلها، أو استئجار محام متضلع فيها، ثم صنع دليل تفصيلي عن كيفية الاستفادة بدقة من الثغرات في القانون⁽⁶⁾. هناك الكثير من الثغرات، ويحيد كثيرون من محامي الدفاع العثور على طريقهم بواسطتها. وعلى رغم ذلك، لا يتوقف عمل الشرطة، وينجح باستمرار في إلقاء القبض على المجرمين وإدانتهم⁽⁷⁾.

وبصورة أعم، فإن معظم ما يتعلق بالشرطة ومكافحة الجريمة معلن للعموم. نعرف ميزانيات قوى الشرطة في البلاد كلها. نعرف قدراتها. نعلم مدى فعاليتها. نعرف ما تفعله ومدى كفاءتها في ذلك. لا نعرف هوية ضباط الشرطة السريين، لكننا نعرف عموماً كيف يُستخدَمون، وما يستطيعون الإقدام عليه، وما لا يستطيعون. كل تلك الأمور معلنة، ويعرفها جيداً أولئك الذين يعطون الشرطة سلطة على الناس، مثلما يعرفها من يخطط لارتكاب جرائم. وعلى الرغم من ذلك، تستطيع الشرطة دوماً التصدي للجرائم.

يبرهن ذلك على أن المستوى الحالي من السرية في العمل ضد الإرهاب مبالغ به. إذ يطبق مستوى عسكري من السرية على ما عُدّ دوماً شأنًا محلياً. لا يفوق الإرهابيون المجرمين ذكاءً. ولا يوقع الإرهابيون قتلى وخراباً أكثر مما يفعل المجرمون، ويتلخص الأمر في أننا نخشى الإرهاب أكثر⁽⁸⁾. يلزمنا نقل مبادئ الشفافية من القوى التقليدية لإنفاذ القانون إلى الأمن القومي، بدلاً من زيادة السرية حول قوى إنفاذ القانون، على نحو ما شرعنا به فعلياً بكل أسف. يجب أن نصنع نظماً رقمية تبقي علينا آمنين، حتى عندما تكون تفاصيلها علنية ومعروفة من العدو⁽⁹⁾. بات حفظ الأسرار أشد صعوبة اليوم، ونكون في وضع أفضل إذا قللنا الأسرار عدداً.

في ثمانينيات القرن العشرين، أوقفت الولايات المتحدة مساعيها لجعل بحوث التشفير سرية؛ لأن نتيجة تلك المساعي كانت الإساءة إلى مهندسينا وعلمائنا في

الرياضيات، بالمقارنة مع أقرانهم في بلدان أخرى⁽¹⁰⁾. وفي وقت قريب، أوقفت الولايات المتحدة مساعيها لجعل بحوث تصنيع الفيروسات البيولوجية سرية؛ لأن أحداً ما سينشر تلك المعلومات بغض النظر عما نفعه. ويدرك المفكرون العسكريون حاضراً أنّ كثيراً من الأسرار العسكرية الاستراتيجية يصعب حفظها؛ بسبب القدرات الشاملة للتصوير بالأقمار الاصطناعية وما يشبهها من التقنيات⁽¹¹⁾. يجدر التفكير بشأن السرية الحكومية في ما يتصل بالرقابة، بطرق مشابهة لما ورد أعلاه.

توجد قوانين لشفافية الرقابة في الولايات المتحدة. في نصه الأصلي للعام 1968، تطلب قانون التنصت على خطوط الهاتف أن تقدّم الحكومة تقارير علنية مكثفة عن استخدامها للتنصت. وتضمّنت تقارير بحجم 200 ورقة سنوياً عن التنصت الهاتفي كميات ضخمة من التفاصيل. أتاح ذلك للناس التثبت مما يفعله مكتب الـ «إف بي آي»، والتأكد من عدم إساءته لسلطاته. ظهرت المشكلة مع التوسع في الأشكال الأخرى من الرقابة بعد 9/11، مع عدم تطلب تقارير مماثلة. يجب إصلاح ذلك الخلل.

يجب على الحكومة الأميركية نشر توصيف تفصيلي غير سريّ عن أمدية تجميع المعلومات الاستخباراتية ودرجة اتساعها. وكذلك نشر تبريرات قانونية لبرامجها في الاستخبارات. ويجب أن تنشر معلومات عن نوع البيانات التي تجمعها سلطاتها المختلفة وكميتها، إضافة إلى معلومات عن عمليات التقليل وقوانين الاحتفاظ بالبيانات. كما يجب عليها نشر الآراء العامة لمحاكمة «فيسا»^(*) التي تشرف على نشاطات الرقابة لـ «وكالة الأمن القومي» بموجب قانون «فيسا» وتعديلاته. يفرض القانون الإبقاء على أسماء الناس والمنظمات الخاضعة للترصد، لكنه لا يفرض ذلك بالنسبة للتشريعات التي تعمل تحتها منظمات الرقابة.

(*) انظر الفصل الخامس.

إشراف أكثر وأفضل

السيطرة على رقابة «وكالة الأمن القومي»، نحتاج إلى تحسين وزيادة الإشراف على الاستخبارات القومية وقوى إنفاذ القانون معاً.

يأتي الإشراف الاستراتيجي أولاً. إذ برّرت «وكالة الأمن القومي» أفعالها دوماً بالإشارة إلى إشراف الكونغرس عليها⁽¹²⁾. وزعم قادتها أن موظفي الوكالة بالكاد انصاعوا للقوانين التي صاغها الكونغرس أو الأوامر التي وقّعها الرئيس. ووفقاً لأحد بياناتها الصحافية الرسمية، «تمارس «وكالة الأمن القومي» نشاطاتها كافة بالتوافق مع ما هو مطبق من القوانين والتوجيهات والسياسات». ليس ذلك صحيحاً البتّة، بل يحمل خداعاً عميقاً. ونعرف من وثائق أُسقطت سرّيتها أخيراً عن آراء «محكمة فيسا»، خصوصاً تلك التي كتبها القاضي جون بايتس، أن «وكالة الأمن القومي» قدّمت تشخيصات خاطئة إلى المحكمة، ولم تنصع لمتطلبات التقليل [في مدى نشاطاتها المجازة] وتجاوزت تكراراً تفويضاتها القانونية⁽¹³⁾.

تلاعبت «وكالة الأمن القومي» بالقوانين التي تضبط إشراف الكونغرس عليها؛ كي تضمن عدم حدوث تفهّم حقيقي أو مراجعة حاسمة⁽¹⁴⁾. وتكوّنت الوثائق التي قدّمتها الوكالة للكونغرس إما من نصوص دعائية مُصمّمة بهدف الإقناع، أو وثائق مملوءة باللغة التقنيّة بهدف إحداث التباس. كما لا يتمكن أعضاء الكونغرس من تحريك تلك الوثائق من الغرف المؤمّنة التي تحزّن فيها، ولا يستطيعون إزالة الملاحظات التي يكتبونها⁽¹⁵⁾. جلّ ما يستطيعه أعضاء الكونغرس هو استقدام موظفين مأذون لهم أمنياً؛ كي يشرحوا لهم معنى تلك النصوص ودلالاتها، مع ملاحظة أنّ قلة من صنّاع التشريع لديهم موظفون يجوزون أذونات أمنية متقدّمة المستوى ولديهم خبرة ملائمة⁽¹⁶⁾. ويضاف إلى ذلك أن الوكالة مارست ضغوطاً كثيفة عليهم⁽¹⁷⁾. إذ صرّح السيناتور رون وايدن أن المسؤولين الكبار في الاستخبارات قدّموا «تصريحات مضلّلة أو مخادعة» في لجان الاستماع في

الكونغرس. وكذلك استتجت السيناتورة ديانا فاينشتاين، رئيسة «اللجنة المختارة من مجلس الشيوخ عن الاستخبارات»، أن لجنتها ويكل أسف «لم تكن تُخبر بطريقة مناسبة»⁽¹⁸⁾ من مجتمع الاستخبارات عن نشاطاته، على الرغم من الانحياز المديد لفاينشتاين لمصلحة الرقابة الحكومية. وسمى آلان غرايسون، عضو الكونغرس عن فلوريدا، إشراف الكونغرس على «وكالة الأمن القومي» بأنها «نكتة»⁽¹⁹⁾.

في العام 2014، دعاني 6 أعضاء في الكونغرس من الحزبين الجمهوري والديمقراطي لعرض خلاصة عن نشاطات الوكالة⁽²⁰⁾. ولأنني راجعت مجموعة كبيرة من وثائق سنودن غير المنشورة، كنت أعرف عن نشاطات الوكالة أكثر منهم. كيف يمكن لديمقراطيتنا أن تستمر إذا كانت أفضل المعلومات التي يستطيع الكونغرس معرفتها، آتية مني؟

من ناحية أخرى، لا يرغب بعض المُشرّعين بممارسة مهمة الإشراف المناطة بالكونغرس. يرجع بعض التلكؤ إلى الرغبة في الإنكار السعيد. ويكون الأمر أكثر أماناً في السياسة، عندما يترك للسلطة التنفيذية مهمة صنع القرارات، إذا فلتنصب سيول الحرارة على تلك السلطة عند حصول أمر سيئ. وثمة مغامرة سياسياً في الوقوف بوجه قوى إنفاذ القانون⁽²¹⁾. وبالنتيجة، لم تغامر سوى قلة من أعضاء لجنة فاينشتاين بالذهاب إلى الغرف الأمنية في «وكالة الأمن القومي».

تفسّر الوكالة سلطاتها بشراسة كأنها تصارع من أجل النجاة بنفسها. في الفصل 5، ناقشت ثلاث سلطات مختلفة تستخدمها الوكالة لتبرير نشاطاتها في الرقابة: الأمر التنفيذي رقم 12333، والبند 215 من «قانون باتريوت» والبند 702 من «قانون تشريعات فيسا».

يتميّز الأمر التنفيذي 12333، وهو وثيقة رئاسية للعام 1981 يأذن للوكالة بمعظم نشاطاتها الرقابية، بأنه متسامح معها إلى حدّ لا يصدّق⁽²²⁾. ويُفترض أنه يسمح للوكالة بممارسة الرقابة خارج الولايات المتحدة، لكنه يعطي الوكالة أيضاً

سلطة واسعة لجمع بيانات عن أميركيين⁽²³⁾. ولا يقدم سوى حماية قانونية واهية للبيانات التي تُجمع عن أميركيين خارج بلادهم، وأقل منها كثيراً بالنسبة للبيانات التي تجمع مصادفة عن مئات ملايين الأميركيين. ولأنه توجيه رئاسي وليس قانوناً، لا تملك المحاكم سلطة حياله، كما لا يمارس الكونغرس سوى الحد الأدنى من الإشراف عليه. يضاف إلى ذلك، على الأقل في 2007، اعتقد الرئيس أنه يستطيع تعديله أو تجاهله، سرّاً ووفقاً لإرادته⁽²⁴⁾. وبالنتيجة، لا نعرف سوى القليل جداً عن كيفية تفسير الأمر التنفيذي 12333 من قبل «وكالة الأمن القومي».

لم يقصد بالبند 215 من «قانون باتريوت» أن يكون تفويضاً برقابة عامة، ومن الممكن إعطاء حجج قوية للقول إن لغته لا تجيزها. إذ كانت الفكرة هي تمكين الـ «إف بي آي» من الحصول على معلومات «لها دلالتها بالنسبة لتحقيق [من الأمن القومي] يكون مرخصاً به قانونياً» - بمعنى أنه تحقيق له موضوع محدد - يحصل على معلوماته من مصادر واسعة، لم يكن بوسع الوصول إليها قبل ذلك. وضربت الرئاسة مثلاً بمعلومات عن كُتب حصل عليها شخص مشتبّه فيه من مكتبة، ربما قرأ «المُرشد العملي للفوضوي» أو ما يشبهه⁽²⁵⁾. في الواقع، أثناء نقاش مشروع ذلك القانون، كان يشار إليه باسم «الشرط بصدد المكتبة». واقتصر شأنه على تمكين مكتب الـ «إف بي آي» من طلب معلومات كان بمكتبته الحصول عليها بواسطة مذكرة قضائية من محكمة كبرى - مع الاقتصار على «البيانات الوصفية»، وليس المحتوى - فأتاح للـ «إف بي آي» الحصول على المعلومات عينها من دون انعقاد محكمة. بدا ذلك منطقياً؛ لأنه لا توجد فعلياً محكمة كبرى بشأن تحقيقات الأمن القومي.

أياً كان الأمر، فعندما أقرّ «قانون باتريوت» في 2001، غرّبل محامو الأمن القومي في وزارة العدل القانون بحثاً عن ثغرات فيه. وعلى الرغم من أن القانون قصد تسهيل المراقبة الموجهة، قرّر أولئك المحامون أنه بالمستطاع توسيع حدوده ليكون تخوياًً بالرقابة العامة. وعلى الرغم من أنه أعطى تمكيناً للـ «إف بي آي»

وحده، فإنهم قرّروا أنّ ذلك المكتب يستطيع أن يطلب نقل المعلومات إلى «وكالة الأمن القومي». في البداية، فعلوا ذلك من دون موافقة أي محكمة على الإطلاق. وبالنتيجة، قرّروا أن تنظر مسائلهم أمام «محكمة فيسا» السريّة⁽²⁶⁾. وفي غياب من يقدم رأياً معارضاً، كانوا قادرين على إقناع القاضي بأن كل ما يفعلونه له «دلالة» بالنسبة لتحقيق ما. كان ذلك تفسيراً جديداً لمعنى كلمة «دلالة»، وهو تفسير لا يستطيع اجتياز أبسط تدقيق. إذا كانت كلمة «دلالة» ليس بمقدورها أن تفرض حدوداً على تجميع المعلومات لأن كل شيء له دلالة، فلماذا أصلاً وُضع ذلك التقييد في القانون؟ حتى عضو الكونغرس جيم سنسبرينر الذي تولى صياغة «قانون باتريوت»، تولّته الدهشة عندما علم أن الوكالة استخدمت ذلك القانون لتبرير جمع معلومات بفرضها رقابة عامة على الأميركيين⁽²⁷⁾. ووصف ذلك بقوله: «يشبه الأمر اغتراف المحيط لضمان التقاط سمكة»⁽²⁸⁾.

البند 702 من «قانون تشريعات فيسا» له قصة مختلفة قليلاً. إذ افترض أن ذلك التشريع يقدر على حلّ مسألة محدّدة. يلجأ مسؤولو الإدارة الرئاسيّة إلى رسم الإشكال التالي: يتحدّث إرهابي من السعودية مع إرهابي في كوبا، والبيانات تتدفق عبر الولايات المتّحدة لكن يُفترض بـ «وكالة الأمن القومي» ألا تنتصّت إلا خارج بلادها. ويحتاج المسؤولون بأنّ ذلك يمثل أمراً غير فعّال، وسمح البند 702 للوكالة بأن تلتقط مكالمات من خطوط تمرّ في الولايات المتّحدة.

مرة أخرى، لا شيء في البند 702 يحوّل فرض رقابة عامة. وتبرّر الوكالة استخدامه بإساءة استعمال كلمة «عرضي». إذ يجري اعتراض كل شيء، «البيانات الوصفية» والمحتوى معاً، ويفتش أوتوماتيكياً بهدف العثور على عناصر مهمّة للوكالة. تزعم الوكالة أن الأشياء التي تسعى إلى تخزينها تملك أهلية اعتبارها بحثاً. وتصنّف الأشياء الأخرى كلها بوصفها «عرضية»، وطالما أن «الشخص - الهدف» المطلوب هو خارج الولايات المتّحدة، فلا بأس في ذلك. هناك تشبيه مجدّ لتلك الصورة يتمثّل في السماح لضباط الشرطة بتفتيش بيوت المدينة كلها بحثاً عن

شخص يعيش طبيعياً في بلغاريا. في تلك الحال، يحتفظ الضباط بها يصادفونه عرضاً من أدلة عن أي جريمة، ثم يحاججون بأن عمليات التفتيش الأخرى يجب أن لا يتم احتسابها تفتيشاً لأنها لم تعثر على شيء، وأن ما عثروا عليه يجب قبوله كدليل لأنه الثَّقُط «عرضياً» أثناء البحث عن البلغاري. يمنع التعديل الرابع في الدستور الأميركي ذلك النوع تحديداً، ويصنّفه كـ «غير منطقي»، ولأسباب وجيهة تماماً.

أظن أنه عندما ظهر «قانون تشريعات فيسا» في 2008، كانت «وكالة الأمن القومي» على وعي تام بما تفعله، لذا عمدت إلى إعمال مطرقها بكلمات ذلك القانون كي تفسح المجال أمام تفسيرها الخاص له. ولربما قدّمت قيادتها خلاصات للجان الاستخبارات في مجلسي النواب والشيوخ، عن قراءتها لنصوصه. ومن المؤكّد أنها لم تخبر جميع أعضاء المجلسين، وكذلك الشعب الأميركي. أعتقد أن كثيراً من تلك الأفعال سوف يتبيّن مخالفتها للدستور. إذ يحمي التعديل الرابع في الدستور الأميركي من عمليات التفتيش غير المنطقية، ومن المصادرات غير المنطقية أيضاً. وبعدّ مجرد الحصول على نسخة من الكتلة الرئيسة لبيانات شركات كـ «فريزون» (Verizon)، مصادرة غير قانونية أيضاً.

تتمثّل المشكلة في أن السلطات التشريعية والتنفيذية والقضائية تخلّت عن سلطاتها في الإشراف. في المسار الديمقراطي الطبيعي، يجري تحويل قانون ما إلى قواعد تتحوّل بدورها إلى إجراءات عملية؛ ما يجعل كل خطوة عرضة للتفسيرات، وهو أمر يفرض وجود إشراف مستمر بواسطة تلك الخطوات كلها. من دون ذلك الإشراف، يحتمل أن تسيء الوكالات الحكومية استخدام سلطاتها. حدث ذلك في سبعينيات القرن الماضي، عندما تجسّست «وكالة الأمن القومي» والـ «إف بي آي» على الأميركيين ضمن مشروعين سُمّيّا «شامروك» (SHAMROCK) و«مينارت» (MINARET)، إضافة إلى مشروع لم تجر تسميته وكان جزءاً من الحرب على المخدرات. ويتكرّر ذلك حاضراً⁽²⁹⁾.

ليس الأمر ظاهرة أميركيّة حصريّاً. حدث الأمر عينه في المملكة المتحدة عام 2000، عند تبني «قانون تنظيم سلطات التحقيق»⁽³⁰⁾. إذ استخدمت «القيادة الحكوميّة للاتّصالات»، وهي النظير البريطاني لـ «وكالة الأمن القومي»، البند 16 (3) الذي جرى إغفاله إلى حد كبير عند نقاش القانون، كي تتجسّس على مواطنين بريطانيين. وعمليّاً، استُبعد البند من النقاش، بل استشرس بعض البرلمانيين دفاعاً عن صياغته الغامضة والمتوترة عمداً⁽³¹⁾، التي لم تكن عمليّاً تحيز الرقابة العامة، ولم يحل ذلك دون الوصول إلى استخدام ذلك البند مبرراً للرقابة العامة⁽³²⁾. وشخصيّاً، اعتقد أن فكرة البند 702 في «قانون تشريعات فيسا» جاءت من البند 16 (3) في «قانون تنظيم سلطات التحقيق».

في العام 2013، حاول الرئيس أوباما طمأنة الأميركيين بأن برامج الرقابة في «وكالة الأمن القومي» تخضع للمراجعة، وتتطلّب موافقة الأذرع الثلاث للحكم⁽³³⁾. لم يكن خطابه سوى تضليل⁽³⁴⁾. قبل كشوفات سنودن، لم تعرف بالمدى الكامل لنشاطات الرقابة الحكوميّة سوى قلة من أعضاء السلطة التنفيذية، وكُشفت جزئياً لبعض الأعضاء الرفيعي المستوى في السلطة التشريعيّة، ولم تُحرز تشريعاً إلا من قبل محكمة «فيسا» التي رفضت 11 من أصل 34 ألف طلب للتفويض تقدّمت بها «وكالة الأمن القومي»، في الفترة الممتدة بين تأسيس «فيسا» في 1979 والعام 2013. لا يعبر ذلك عن إشراف فعلي. وإنصافاً، يظل ذلك إشرافاً أكبر مما يحدث في بلدان كثيرة، بما فيها بلدان ديمقراطيّة كفرنسا وألمانيا وبريطانيا.

يحاول بعض أعضاء الكونغرس فرض قيود على الوكالة، ويمكن لبعض مقترحاتهم أن يكون مؤثراً، بل يصنع فارقاً في عمل الوكالة. وعلى الرغم من ذلك، لا يحدوني الأمل بأن يقوم الكونغرس حاضراً بإصلاح مُجدٍ؛ لأن كل المقترحات المتعلّقة بالوكالة تركز على برامج وسلطات محدّدة. إذ تتناول تلك المقترحات مثلاً برنامج الوكالة لجمع «البيانات الوصفية» تحت البند 215⁽³⁵⁾، والتجميع الواسع للتسجيلات تحت البند 702 وهكذا دواليك⁽³⁶⁾. لا تستطيع تلك المقاربة المجزأة

أن تكون فعالة. لقد تجاوزنا مرحلة أن يستطيع تدخل تشريعي بسيط أن يُحدث فارقاً. وحاضراً، هناك كثير من السرية في عمل الوكالة، كما تتناقل مجموعة من برامجه تبريرات قانونية متنوعة⁽³⁷⁾. عندما ترفض الشركات رسائل الوكالة، ترميها الحكومة بأمر يستند إلى البند 215⁽³⁸⁾. وتكراراً، هددت الوكالة بأنه إذا قلّص الكونغرس صلاحيتها المستندة إلى البندين 215 و 207، فسوف تنقل البرامج المُقلّصة إلى صلاحية الأمر التنفيذي رقم 12333 المتسم بتسامح أكبر معها، إضافة إلى كونه أقل سيطرة ويتمتع بسرية كبيرة⁽³⁹⁾.

ثمة محاولات أخرى للإشراف. في العام 2013، شكّل الرئيس أوباما لجنة مراجعة لـ «وكالة الأمن القومي»، حازت سلطات كبيرة في النفاذ إلى نشاطات الوكالة وقدراتها. وأنتجت اللجنة تقريراً ممتازاً تضمّن 46 توصية بشأن سياسة الوكالة⁽⁴⁰⁾، كما وافق الرئيس أوباما على تنفيذ مجموعة كبيرة منها⁽⁴¹⁾. يبقى السؤال عما أنجزه الرئيس فعلياً. في العام 2004، أنشأ الكونغرس «هيئة الإشراف بصدد الخصوصية والحريات المدنية» بتوصية من «لجنة التحقيق في 9/11»، بهدف الإشراف على قضايا الأمن القومي⁽⁴²⁾. افتقرت اللجنة إلى عدد كافٍ من الموظفين، كما لم تنل تمويلاً مناسباً، حتى العام 2012، ولم تحز سوى القليل من السلطات. (قدّمت الهيئة تقريراً في 2014، اكتفى بالتركيز على تجميع الوكالة للمعلومات تحت البند 702⁽⁴³⁾. وحُظِرَ على نطاق واسع بدعوى أنّه غير مناسب)⁽⁴⁴⁾.

يجب أن يكرّس عدد أكبر من أعضاء الكونغرس أنفسهم لمهمة إصلاح «وكالة الأمن القومي» بشكل مفيد. إذ نحتاج إلى إشراف استراتيجي شامل على الوكالة يكون متّسماً بالشفافية التامة، تنهض به وكالات حكومية مستقلة. نحتاج إلى قوانين مؤثرة من شأنها تقليص تجميع البيانات عن الأميركيين وتخزينها، إضافة إلى قوانين تفرض على الوكالة حذف المعلومات التي كان يجب ألا تجمعها أصلاً⁽⁴⁵⁾. في سبعينيات القرن العشرين، حقّقت «لجنة شيرش» في عمليات جمع المعلومات استخباراتياً من قبل «وكالة الأمن القومي» والـ «إف بي آي» والـ «سي آي إيه»:

واستطاعت إنجاز إصلاح في تلك الأجهزة، بعد بحوث وكشوفات واسعة. نحتاج إلى لجنة كتلك حاضراً. يجب علينا إقناع الرئيس أوباما بتبني التوصيات التي خرجت بها لجنته التي راجعت عمل «وكالة الأمن القومي». ويجب إعطاء سلطات تحقيق فعلية إلى «هيئة الإشراف بصدد الخصوصية والحريات المدنية».

تحمل تلك الاقتراحات كلها دلالة بالنسبة إلى الإشراف الاستراتيجي على الرقابة العامة. إذًا، لننتقل إلى الإشراف التكتيكي. تجسّد عملية الحصول على مذكرات قانونية إحدى الآليات المهمة في الإشراف التكتيكي على الرقابة الحكومية. وعلى عكس مزاعم يرددها بعض المسؤولين الحكوميين، لا يتأذى الأمن القومي من المذكرات القانونية؛ بل إنها آلية أمنية تحمينا من التمدد الزائد لسلطات الحكومة⁽⁴⁶⁾.

ولا تتمتع الأذونات الأمنية السرية بفعالية ماثلة⁽⁴⁷⁾. يأتي القضاة الذين يشرفون على عمل «وكالة الأمن القومي» من محكمة «فيسا» السرية. وبالمقارنة مع المحاكم التقليدية، تمتلك «فيسا» مستوى أقل بكثير في الاستناد إلى الأدلة قبل إعطاء إذن أمني. وتضرب ستاراً من السرية على الحالات التي تنظرها، والأحكام التي تصدرها، كما لا تستدعي أحداً ليمثل الطرف الآخر أمامها. ومع أخذ عدم التوازن في تلك الآلية بعين الاعتبار، يغدو مدهشاً التماسك الذي أظهرته محكمة «فيسا» في مواجهة الوكالة (على الرغم من أنها لم ترفض إعطاء إذن للوكالة إلا نادراً).

يتخطى بعض أوامر الرقابة تلك الآلية كلياً⁽⁴⁸⁾. إذ لم تتلق مؤسسة «الاتصالات الخلوية» في الولايات المتحدة سوى أمرين قضائيين للتفتيش على الخطوط، مقابل 10801 مذكرة تفتيش لم تكن مستندة إلى القضاء إطلاقاً. يجب إصلاح تلك الأمور كلها.

لنبدأ من محكمة «فيسا»: يجب أن تصبح أشد علانية بكثير⁽⁴⁹⁾. يجب أن يتولى مجلس الشيوخ تعيين كبير القضاة في تلك المحكمة. يجب أن تشر المحكمة آراءها إلى أقصى حدّ تستطيعه. يفترض تعيين محام للدفاع عن مصالح الجمهور كي يحاجج

ضد طلبات تطبيق الرقابة. يفترض بالكونغرس أن يسنّ آلية لاستئناف الأحكام الصادرة عن «فيسا»، إما أمام محكمة نقض مختصة أو المحكمة الفيدرالية العليا.

هناك حاجة أيضاً لاتباع مزيد من الخطوات لوضع «وكالة الأمن القومي» تحت إشراف تكتيكي موثوق⁽⁵⁰⁾. إذ تميل الإجراءات الداخلية للوكالة للتلاؤم مع تقصي نشاطات كالرقابة غير الصحيحة والقبالة للتجنّب أكثر من اهتمامها بآليات الرقابة التي تسعى إلى كشف من يحاولون التملّص من الرقابة، سواء أكانوا أفراداً أم منظمات بأكملها. إنّ وجود مراقب خارجي شيء أساسي لتصحيح ذلك. ومن المهم أيضاً أن يضحّي الرسميون الحكوميون مسؤولين بصفة شخصية عن سلوكيات الوكالة المتعدية وغير الشرعية. لم يطرد متلصّص من مجموعة «لوف إنت» في الوكالة، ناهيك عن عدم محاكمتهم.

كذلك صُدّت محاولات سنودن المتكررة داخل الوكالة للتعبير عن قلقه بشأن المدى الذي بلغته الرقابة على الأميركيين⁽⁵¹⁾.

تملك وكالات حكومية أخرى تعمل على إنفاذ القانون، كالـ «إف بي آي»، آليات للإشراف الداخلي⁽⁵²⁾. في ذلك المجال أيضاً، كلما زادت الشفافية تصبح الأمور أفضل⁽⁵³⁾. لطالما منحنا الشرطة صلاحيات استثنائية بهدف تقصي الجرائم. فعلنا ذلك عن سابق معرفة، وهو ما جعل المجتمع أكثر أماناً؛ لأنه بإمكاننا دوماً ضبط تصرفات الشرطة بموجب القوانين، كما يمكن اللجوء إلى أنواع معروفة من التقاضي في حال أساءت الشرطة استعمال سلطاتها. من المستطاع النقاش مطوّلاً عن مدى نجاعة ذلك المسار عملياً في الولايات المتحدة ودول أخرى، لكن تبقى الفكرة الأساسية سليمة.

حماية مُطلق صافرات الإنذار

يدعم البروفسور ديفيد بوزن، وهو أستاذ القانون من «جامعة كولومبيا»، فكرة أن النُظم الديمقراطية يجب أن تكون مُسرّبة، عَادًا التّسريبات وإطلاق صافرات الإنذار آليات أمنيّة بحد ذاتها، تتصدى للتوسّع الفاضل في سلطات الحكم⁽⁵⁴⁾. وكذلك يرى أن التّسريبات تمثل نقيضاً لميل السلطات الرسميّة إلى الإفراط في وضع الوثائق في خانة السّريّة؛ ما يجعل التّسريبات في خاتمة المطاف طريقة لاسترداد الثقة بالحكومات، بعد تضرّرها من تأثيرات السّريّة الزائدة.

كذلك تنظر عالمة الإثنيات دانا بويد إلى إطلاق صافرات الإنذار بوصفها شكلاً للتمرد المدني في العصر الرقمي؛ لأنّه يعطي قوّة للأفراد في مواجهة إساءة استخدام السلطة⁽⁵⁵⁾. ولاحظت منظمة «مراقبة حقوق الإنسان» (Human Rights Watch) غير الحكوميّة، أن «الأشخاص الذين يكشفون ممارسات رسميّة خاطئة... يؤدّون خدمة جليّة في المجتمع الديمقراطي...»⁽⁵⁶⁾.

ووفق هذه الطريقة في التفكير، يقدّم مُطلق صافرات الإنذار آلية أخرى للإشراف على الحكومة⁽⁵⁷⁾. من المستطاع اعتبارهم نوعاً من التفتيش المفاجئ العشوائي. وعلى غرار القوانين التي تحمي مُطلق صافرات الإنذار ضد الشركات، كذلك يجب سنّ قوانين تحمي مُطلق صافرات الإنذار ضد الحكومة⁽⁵⁸⁾. ولدى إقرارها، نحصل على إطار وقوانين لإطلاق صافرات الإنذار بطريقة شرعيّة⁽⁵⁹⁾.

ولا يعني ذلك أن يضحي كل شخص حرّاً في تسريب وثائق حكوميّة بدعوى أنّه مُطلق صافرة إنذار. في المقابل، يعني ذلك تماماً أن كشف أخطاء الحكومة بدافع من الضمير، يمكن اتّخاذ سنداً قانونيّاً يستخدمه مُطلق صافرة الإنذار عند مثولهم أمام المحاكم - يبقى على القضاة الحكم على صحة مبرراته - إضافة إلى تمكينهم من الحفاظ على سريّة مصادره. هناك نقطة ذكيّة في هذه الصيغة تتمثّل في تنحية الإشكاليّة الصعبة التي يشكّلها تعريف «مُطلق صافرة إنذار»، إضافة إلى

تمكين المحاكم من التحديد في كل حال على حدة، الأفعال التي ينطبق عليها ذلك الوصف⁽⁶⁰⁾. بذا، يستطيع شخص كسنودن أن يعود إلى الولايات المتحدة ويقدم قضيته إلى المحاكم⁽⁶¹⁾، وهو أمر يتعذر عليه حاضراً وفق ما بينت في الفصل 7.

إضافة إلى ذلك، نحتاج إلى سنّ قوانين تحمي الصحفيين في حال تمكنهم من الوصول إلى معلومات مصنفة سرية. إذ لا يمثل كشف الأمور علانية عملاً تجسسياً بحد ذاته، ومعاملة الصحافة كأنها جاسوسية أمر مؤذٍ للديمقراطية، بطريقة نفوق المؤلف تماماً.

في الفصل السابع، تحدثت عن حماسة فائضة لدى إدارة أوباما في اضطهاد مُطلق صافرات الإنذار. تجمع تلك سياسة الرياء والخطورة معاً. إذ نشجع الأفراد على إطلاق صافرات الإنذار بشأن تجاوز القانون من قِبل القطاع الخاص، ولكننا نحتاج إلى قوانين مماثلة بشأن الحكومة أيضاً⁽⁶²⁾.

تضييق الاستهداف وحصره بالموافقة القانونية

تشكل الرقابة الإلكترونية أداة قيمة بالنسبة لقوى إنفاذ القانون وتجميع المعلومات الاستخباراتية معاً، لذا يفترض أن نستمر في استخدامها. هناك مشكلة في فرض رقابة إلكترونية على أمة بأكملها، خصوصاً الرقابة العامة التي لا تتقيد بأوامر القضاء. وكما رأينا في الفصل 11، لا تجعلنا تلك الرقابة أكثر أماناً. وفعلياً، إنها تقلل من أماننا بأنها تحرف الاهتمام والأموال عن الوصول إلى أشياء تجعلنا أكثر أماناً حقاً. يتمثل الحل فعلياً في العودة حصرياً إلى الرقابة الموجهة.

وفق كلمات أكسل آرنباك وهو باحث في القانون والأمن السبراني، يتحكم القانون بالأبواب الأمامية، وتسيطر نظرية الألعاب (*) على «الأبواب الخلفية»⁽⁶³⁾.

(*) في أربعينيات القرن الماضي، صاغ عالم الرياضيات الأمريكي جون ناش نظرية عن حساب المخارج المحتملة لأشكال متنوعة من الصراعات، تشمل الاقتصاد والجيش والاقتصاد والعلاقات الاجتماعية.

وقصد آرباك القول إنّ عملية الرقابة الموجهة تتحكم بها عناصر كالسبب المحتمل، المذكرات القضائية، محدودية الإطار وغيرها من القوانين التي تحمي أمننا وخصوصيتنا. وتتحكم بالرقابة العامة التحليلات الباردة عما تستطيع المؤسسة جمعه من المعلومات، وطُرق الإفلات من تبعات ذلك. عندما نعطي «وكالة الأمن القومي» القدرة على تنفيذ رقابة عامة بالتملص من آلية المذكرات القضائية، نتيح لموظفي الوكالة التفكير أكثر في ما يستطيع جمعه من معلومات، والتفكير أقل في مدى قانونيته. عندها، نفسح لهم المجال ليكونوا طامعين ومتعجرفين؛ وندفع ثمن ذلك.

تقلب رقابة المجاميع عملية التحقيق التقليدية رأساً على عقب. وفي ظلّ الإيقاع الطبيعي للعمليات، لا بد لقوى إنفاذ القانون من سبب كي تشبه بشخص ما، وكذلك لتتقدم بطلب مذكرة قضائية لوضعه تحت الرقابة. ونفسح رقابة المجاميع المجال أمام قوى إنفاذ القانون لرقابة الجميع - وصنع أرضيات للاشتباه. إنّها أمور نص الدستور الأميركي صراحة على منعها، ولأسباب وجيهة تماماً. ولذلك أيضاً، استنتج تقرير الأمم المتحدة في 2014 أنّ الرقابة العامة تهدد القانون الدولي⁽⁶⁴⁾.

نحن بحاجة إلى تشريعات ترغم وكالات الاستخبارات وقوى إنفاذ القانون على جعل رقابتهم موجهة؛ بل نحتاج إلى سنّ تشريعات جديدة وتدعيم التشريعات القائمة معاً سوياً. بفضل ذلك المزيج، تحصل قوى إنفاذ القانون على ما تحتاجه من معلومات بصورة محدّدة، وكذلك تحصل الوقاية من إساءة استخدامها.

خطّت المحكمة العليا في أميركا خطوة طفل صغير في ذلك الاتجاه في 2013، عندما اشترطت حصول ضباط الشرطة على مذكرة قضائية قبل وضع أداة إلكترونية مرتبطة بنظام الـ «جي بي إس» في سيارة المشتبه فيهم⁽⁶⁵⁾، وتلتها خطوة أخرى في 2014 باشتراط حصول ضباط الشرطة على مذكرة قضائية لتفتيش الهاتف الخليوي للموقوفين والمعتقلين⁽⁶⁶⁾.

في الولايات المتحدة، نحتاج إلى التخلص من نظام الطرف الثالث المتقادم⁽⁶⁷⁾، وأن نقر بأن المعلومات تبقى محتفظة بكونها شخصية حتى لو جرى إيكالها إلى أحد المُقدِّمين الموثوقين لخدمة الإنترنت. يجب أن تضطر الشرطة إلى الحصول على مذكرة قضائية للوصول إلى بريدي الشخصي، سواء أكان مكتوباً على الورق أم إلكترونياً في حاسوبي في المكتب أم في خوادم شركة «غوغل» أينما كانت في العالم⁽⁶⁸⁾.

يملك الكثير من تلك الأشياء طابعاً دولياً. ويتطلب إنجاح ما اقترحته أن تقرّ الحكومات بأنها ملزمة بحماية حقوق مواطنيها وحرياتهم، بل حقوق المواطنين وحرياتهم عالمياً. إنه أمر مستجد تماماً؛ ذلك أن الحماية القانونية في الولايات المتحدة حيال الرقابة، لا تنطبق على غير الأميركيين خارج تلك البلاد. يفترض وضع اتفاقيات دولية تأخذ بعين الاعتبار أن واجبات بلد ما لا تتوقف عند حدوده. هناك مسوّغات أخلاقية أساسية للقيام بذلك، إضافة إلى وجود أسباب براغماتية له. إذ تساعد حماية حق الأجانب في الخصوصية في حماية حقوقنا أيضاً، كما تتأتى الأضرار الاقتصادية التي ناقشتها في الفصل 9 من إيداء تلك الحقوق.

لنصلح معظم الثغرات

وفق ما ناقشته في الفصل 11، ثمة نقاش جارٍ حول وجوب قيام الحكومة الأميركية - تحديداً «وكالة الأمن القومي» و«القيادة العسكرية للفضاء السبراني» - بتجميع ثغرات النظم الإلكترونية، أو العمل على إصلاحها وسدّها. إنها مسألة معقّدة تماماً، وتعطي نموذجاً ساطعاً عن صعوبة الفصل بين الهجوم والدفاع في الفضاء السبراني.

ثمة سباق تسلّح مندلّع في الفضاء الافتراضي للإنترنت حاضراً. إذ يعمل الصينيون والروس وغيرهم على تكديس سجلات عن الثغرات في المواقع والنظم الإلكترونية⁽⁶⁹⁾. إذا تركنا الثغرات مفتوحة، فلربما استطاع بلد آخر كشفها باستقلالية، ما يعطيه القدرة على استغلالها ضدنا وضد حلفائنا. في المقابل، إذا عملنا

على سدّ الثغرات كلها، نفقد سلاحاً مهماً لأننا لن نتمكن من استغلال ثغرات في توجيه ضربة ما في الفضاء السبراني ضد عدو محتمل.

يعتقد بعض الناس أنّ «وكالة الأمن القومي» يجب أن تكشف وتصلح الثغرات كلها⁽⁷⁰⁾. ويزعم آخرون أنّ ذلك يشبه نزع سلاح من طرف واحد⁽⁷¹⁾. أوصت لجنة الرئيس أوباما للتدقيق في «وكالة الأمن القومي» بما يشبه حلاً وسطاً: يجب ألا تكسّر الثغرات إلا نادراً، ولفترة قصيرة⁽⁷²⁾. أثرت تلك النقطة بنفسها⁽⁷³⁾. إذ إنها عين ما تزعم الوكالة، واستطراداً «القيادة الأميركية للفضاء السبراني»، أنها تفعله⁽⁷⁴⁾: إيجاد توازن بين عوامل متنوّعة تشمل إمكان أن يكتشف طرف آخر تلك الثغرات (راجع النقاش عن «نوباس» في الفصل 11)، والأهمية الاستراتيجية لذلك الأمر بالنسبة للولايات المتحدة. في المقابل، تشير الأدلة إلى أنّ ما تكسّسه الوكالة من الثغرات يفوق كثيراً ما تعلن عنه.

تمثّل تلك الحال خطوة إلى الخلف. يجب أن يكون خطأنا في طرف الكشف عن الثغرات. إذ يساعد ذلك البلدان التي تعتمد بكثافة على البنية التحتية للإنترنت كالولايات المتحدة. ويعد ذلك الثقة بالولايات المتحدة بإظهارها رغبتها في وضع الأمن قبل الرقابة. وفي ما يُحتَفَظ بالثغرات وسجلاتها سرّاً، يكون من الأفضل فتح نقاش عن نوع الثغرات التي يجب الإبقاء عليها. ويتطلّب إنجاز ذلك بكفاءة، وجود منظمة حكومية مستقلة تملك خبرات تقنية ملائمة في اتخاذ القرارات.

في السباق على التسلّح الجاري حاضراً، تستثمر المؤسسات العسكرية أموالاً أكثر في البحث عن الثغرات وكذلك في شراء المعلومات عنها، بأكثر مما يوظف عالم التجارة أموالاً في إصلاحها. يحمل تكديس الثغرات وسجلاتها خطراً علينا جميعاً. وبغض النظر عما يفعله مجرمو الفضاء الافتراضي، وما تفعله البلدان الأخرى، يجب على أميركا نقل الخلل إلى الجانب الأمني بإصلاح معظم الثغرات التي نكتشفها، مع

جعل عملية كشفها أكثر علانية. سيجعلنا ذلك أكثر أمناً، مع توليد الثقة بسياسة الولايات المتحدة والمراكز التقنية للإنترنت معاً.

لا تخرب المنتجات والمعايير

تمتلك الثقة أهمية حاسمة للمجتمع؛ وهي شخصية، نسبية، وضعية وسيالة. وتستند عليها إنجازات الشعوب كافة. يجب أن نكون قادرين على الثقة ببعضنا بعضاً، وبمؤسساتنا الحكومية والخاصة، وبالنظم التكنولوجية التي تؤمن وظائف المجتمع. وعندما نبني نظاماً، نحتاج إلى التأكد من كونها أهلاً للثقة بمثل كونها فعالة. وتبدو طبيعة الثقة بالإنترنت أمراً مثيراً للاهتمام. إذ لا يملك المتمرسون بالتقنية أوهاماً بشأن أمن الإنترنت وقدرة الحكومات والمجرمين والـ «هاكرز» وغيرهم على اختراق الشبكات، طالما امتلكوا الدافع والقدرة على ذلك. لا نثق أبداً بأن المبرمجين لا يرتكبون أخطاءً، وأن الشيفرة خالية من العيوب، ولا حتى بمناعة المعادلات الرياضية للشيفرة التي نصوغها بأنفسنا.

إذ نعرف جيداً أن أمن الإنترنت هو سباق تسلح، والمهاجمون يمتلكون معظم الأفضليات.

إن ما نثق به حقاً هو أن التقنيات تصمد أو تنهار ارتكازاً إلى مميزات الخاصة. وبفضل كشوفات سنودن، بتنا نعرف أن تلك الثقة كانت في غير موضعها. وللسبب عينه، ولدت برامج الرقابة لـ «وكالة الأمن القومي» و«القيادة الحكومية للاتصالات»، احتجاجات واسعة عالمياً؛ وثار غضب المجتمع التقني على نحو خاص بسبب ما كشفته وثائق سنودن من تعمد الوكالة تخريب معايير الإنترنت ومنتجاتها وبروتوكولاتها⁽⁷⁵⁾. لقد أضعفت برامج الوكالتين الأميركية ونظيرتها البريطانية الثقة بالتقنية التي تستند إليها الإنترنت.

ناقشتُ في الفصل 6، محاولات الـ «إف بي آي» المستمرة للحصول على قوانين تفرض وضع «أبواب خلفية» خدمة للأمن⁽⁷⁶⁾. وناقشت في الفصل 11، كيف عملت «وكالة الأمن القومي» سرّاً إلى دسّ «أبواب خلفية» في منتجات الإنترنت وبروتوكولاتها، بما يمكنها من ممارسة التجسس. ويفترض أن يذهب بنا الظن إلى أن بلداناً أخرى مارست الشيء نفسه مع منتجاتها (ومع بعضها بعضاً)⁽⁷⁷⁾. واستنتج مراقبون أن شركات لديها طواقم تطوير إسرائيلية، كـ «فرينت» (Verint) و«نارنت» (Narent) و«أمدوكس» (Amdocs)، تنام في السرير عينه مع الحكومة الإسرائيلية، وأنّ معدات شركة «هواوي» (Huawei) متصلة بـ «أبواب خلفية» مع الحكومة الصينية⁽⁷⁸⁾. هل نشق بالمنتجات الأميركية المصنوعة في الصين؟ هل نشق بالمواطنين الإسرائيليين العاملين في شركة «مايكروسوفت»؟ هل نشق بالمكونات الإلكترونية والبرامج الرقمية المصنوعة في روسيا؟ فرنسا؟ ألمانيا؟ هل نشق بأي شيء مصنوع في أي مكان؟

إنّ غياب الثقة سمّ. يجب أن تعطى الأولوية للأمن، وبعده يأتي التنصّت⁽⁷⁹⁾. تستطيع قوى إنفاذ القانون الحصول على مذكرة قضائية لممارسة التنصّت، لكن يجب ألا يكون بمكنتها إرغام شركات الاتصالات على ضمان نجاح كل محاولاتها في التنصّت. يجب استرداد تشريع «كاليا» [الاسم المختصر لـ «قانون مساعدة الاتصالات في إنفاذ القانون»^(*)] وتفعيله بما يجعله يعمل على ضمان أمن شبكات الهاتف والإنترنت.

سيحاول العاملون في قوى إنفاذ القانون على تلك الأمور كلها تخويفنا، باستعادة رؤى الخاطفين والمتغولين جنسياً على الأطفال، وتجار المخدرات، وإفلات الحبل على غاربه للإرهابيين؛ لأنّ قوى إنفاذ القانون لم تعد قادرة على كسر شيفرات كومبيوتراتهم واتصالاتهم. رأينا ذلك في أواخر العام 2014 عندما لجأت شركة

(*) راجع الفصل السادس.

«آبل» إلى تشفير معلومات «آي فون». وحينها، عمد مسؤولو قوى إنفاذ القانون، واحداً تلو الآخر، إلى إثارة أشباح الخاطفين والمعتدين على الأطفال⁽⁸⁰⁾. كانت محاولة متعمدة للعب على وتر الخوف، لكن أحداً من أولئك المسؤولين لم يشر إلى قضية بعينها عن حدوث أي من تلك الأشياء. ومن أصل 3576 اعتداء كبيراً جرى منح إذن قانوني بالتنصت أثناء التحقيق فيها سنة 2013، ظهرت قضية خطف وحيدة لكن ضحيتها لم يكن طفلاً⁽⁸¹⁾. والأهم لم يظهر دليل على أن التشفير يعيق جدياً التحقيقات في الجرائم، بأي طريقة كانت⁽⁸²⁾. في 2013، ضلّل التشفير الشرطة 9 مرات، بزيادة 4 حالات عن 2012، لكن التحقيقات تواصلت بطرق أخرى.

تملك قوى إنفاذ القانون مروحة كبرى من الأدوات الاستقصائية. وتستطيع الحصول على مذكرات قضائية للوصول إلى البيانات المخزنة في السحب الرقمية، ومجموعات ضخمة من «البيانات الوصفية». إنها تحوز القدرة والحق للتسلل إلى حواسيب المشتبه فيهم، بغية الوصول إلى المعلومات التي تحتاجها من دون إضعاف أمننا جميعاً⁽⁸³⁾. إن الأمن الجيد لا يعرضنا للمخاطر.

يجب على مؤسساتنا الأمنية ألا تزرع ثغرات في أي شيء سوى نُظم محدّدة تملكها الحكومات والقوى العسكرية الأجنبية، سواء سرّاً أم علانية، كما يجب عليها التعاون مع المؤسسات الأكاديمية ومجتمعات الأعمال كي تضمن أن الثغرات التي تزرعها أطراف عدوانية سوف تُكشف ويُعلن عنها ويُبطل عملها.

لن نتوصل إلى توافق مع قوى العالم كلّها على عدم تخريب الجزء الذي تسيطر عليه من الإنترنت، لكن يجب علينا التوقّف عن تخريب الأجزاء التي تقع تحت سيطرتنا. تضمّ الولايات المتحدة غالبية الشركات التي تسيّر عمل الإنترنت، ما يعطي أميركا نفوذاً لا يضارع. وبمجرد توقّفنا عن لعبة التخريب، نستطيع توجيه

مواردنا بشكل موثوق إلى تقصي التخريب الذي يحدثه آخرون ومكافحته على الإنترنت، ما يزيد مستويات الثقة عالمياً.

فصل التجسس عن الرقابة

في العام 2013، علمنا أن «وكالة الأمن القومي» تجسست على هاتف المستشارة الألمانية أنغيلا ميركل⁽⁸⁴⁾. علمنا أن الوكالة تجسست على سفارات وبعثات على امتداد العالم: البرازيل، بلغاريا، كولومبيا، الاتحاد الأوروبي، فرنسا، جورجيا، اليونان، الهند، إيطاليا، اليابان، المكسيك، سلوفاكيا، جنوب أفريقيا، كوريا الجنوبية، تاوان، فزويلا، فيتنام⁽⁸⁵⁾. علمنا أيضاً أن الوكالة تجسست على الأمم المتحدة⁽⁸⁶⁾. بالطبع، أرخت تلك الكشوف ظلالها على العلاقات الدولية، لكن هل فاجأت أحداً فعلياً؟ إنَّ التجسس على الحكومات الأجنبية هو عين ما يفترض بالوكالة أن تفعله. إنَّ التجسس المتبادل بين الحكومات قديم قديمَ الحكومات نفسها. إنَّه عمل عسكري مهم في أوقات السلم والحرب، وسوف تستمر أبداً. إنَّه عمل موجه أيضاً. وعملياً، يساهم ذلك في الاستقرار لأنَّه يزيل شكوكاً متبادلة عن نوايا الدول تجاه بعضها بعضاً⁽⁸⁷⁾.

هناك فارق كبير بين التجسس الذي تمارسه «وكالة الأمن القومي» من جهة وبرامجها في الرقابة العامة أميركياً ودولياً من الجهة الثانية. في الفصل 5، لاحظتُ أنَّ تلك النقلة في مهمة الوكالة نجمت من نقلة في مهمتها بشأن مكافحة الإرهاب. فبعد 9/11، أنيط بتلك الوكالة المهمة الرئيسة في الرقابة المتعلقة بمكافحة الإرهاب؛ لأنَّها تمتلك القدرات المطلوبة لتلك المهمة فلا يزيد الأمر على إعادة توجيهها، على الرغم من أن تلك المهمة كان من المستطاع إسنادها إلى الـ «إف بي آي».

ومع توليها مهمة الرقابة لمكافحة الإرهاب، توسَّعت قواعد عملها عسكرياً والإطار القانوني المتصل بنشاطاتها الأساسية في التجسس. وبذا، وجب فرض

السريّة بشأن ممارسة الرقابة على شعوب بأكملها (ومن بينها شعبنا)، تساوي السريّة المفروضة على نشاطاتنا التجسّسية ضد الحكومات.

نحتاج إلى فصل هاتين المهمتين عن بعضهما بعضاً. يجب أن يبقى التجسس الحكومي تحت إشراف وزارة الخارجية والمؤسسة العسكرية. يفترض أن يناط بالرئيس بوصفه القائد الأعلى، تقرير السفارات والهواتف التي يجب التنصّت عليها، كما يفترض بـ «وكالة الأمن القومي» تنفيذ أوامره. ويجب ألا تبرّر غالبية أعمال الرقابة العامة، سواء داخل الولايات المتحدة أم على الأجانب. أحياناً، يمكن تبرير رقابة الحكومة لمواطنين بعينهم، لكن يشترط أن يجري ذلك ضمن تحقيقات جرميّة حصريّاً. ويجب نقل نشاطات الرقابة العامة خارج إطار الوكالة والمؤسسة العسكرية. يفترض بتلك النشاطات أن تكون تحت إمرة الـ «إف بي آي» ووزارة العدل اللتين تتقيدان بقواعد عمل الشرطة على غرار وجود قضيّة محتملة، التزام آلية مناسبة والإشراف على نشاطات الرقابة، ضمن أطر المحاكم العادية العلنيّة.

لا يعني ذلك أن الولايات المتحدة ليست بحاجة إلى إصلاح ضخم لعمل الشرطة. ولقد ناقشت في الفصل 7 مسألة سريّة الشرطة. ثمة مشكلة كبرى تمثّلها العسكرية المتزايدة للشرطة، وكذلك ميل وزارات كثيرة إلى ممارسات تمييزيّة جذريّة⁽⁸⁸⁾. وتصلح تلك الأمور موضوعاً لكتاب آخر⁽⁸⁹⁾. إنّ مكافحة الإرهاب كانت ولا تزال، هي المهمة الرئيسة للـ «إف بي آي».

في كانون ثاني (يناير) 2014، ألقى الرئيس أوباما خطاباً بشأن «وكالة الأمن القومي»، أثار فيه نقطتين بالغتي الأهمية. إذ وعد ألا تستمر الوكالة في رقابة هاتف أنغيلا ميركل. وعلى الرغم من أنه لم يوسّع تلك الهبة لتشمل بقية الـ 28 مليون مواطن ألماني، فإنه أعلن أنه قد يوسّع بعض الحمايات التي يؤمّنها دستور الولايات المتّحدة حيال الرقابة غير المبررة، كي تشمل بقية العالم⁽⁹⁰⁾. وإلى حدّ كبير، يتلاءم

تحقيق هذا الهدف مع وضع رقابة الحكومة على الشعب تحت إشراف مدني، إضافة إلى تقييدها بقواعد عمل الشرطة.

تنظيم دور العسكري في الفضاء السبراني

مثل فصل الحكومة المدنية عن العسكري إحدى الإنجازات الكبرى في الهزيع الأخير من القرن التاسع عشر. وبرهن التاريخ والحوادث السياسية المعاصرة معاً على الدمار الهائل الذي يحق بالمجتمع حين يتولى الجنرالات أمر البلاد. وأعطى الفصل بين السلطين المدنية والعسكرية، وهو ما فعلته بلدان كثيرة عالمياً، مساحة لازدهار الديمقراطية والحرية.

تجسّد المشكلة في أن الفضاء السبراني لا يستطيع بسهولة الفصل التقليدي بين المجالين العسكري والمدني. عندما تتعرّض لاعتداء جسدي، تلجأ إلى منظمات كثيرة للدفاع عنك كالشرطة والجيش وكل من يستطيع الدفاع عنك ضد الإرهاب في بلادك، إضافة إلى محاميك. يعتمد النظام القانوني في تبريره تلك الدفاعات على مرتكزين: من يهاجمك، ولماذا. للأسف، عندما تُهاجم في الفضاء السبراني فإنّ الشئيين اللذين لا تعرفهما هما من يهاجمك ولماذا⁽⁹¹⁾.

إضافة إلى ذلك، لا تملك الإنترنت حدوداً تقارن بالحدود الفعلية بين الدول⁽⁹²⁾ - بل يمكنك القول إنه لا حدود لها إطلاقاً - لذا يصعب التمييز بين الشأين الداخلي والخارجي فيها. إذ تشمل مروحة من يشنون الهجمات مرهقين يسعون لتزجية أوقات الفراغ، ومنظمات إجرامية محترفة، وحتى الدول ومؤسساتها، وربما استخدموا جميعهم التكتيكات والأسلحة عينها، ما يجعل من الصعوبة بمكان التمييز بين أنواع المهاجمين. تحدث الهجمات خلال كسور من الألف من الثانية، وتختلف آثاراً متنوعة.

ويتمثل ردّ الفعل على ذلك بجمع المهاجمين كافة تحت مسمى «الحرب السبرانية»، وهو أمر جديد وجدّي بالنسبة للتخطيط العسكري. وذكرت سابقاً أنّ قرابة 30 بلداً لديها فرق في جيوشها مكرّسة للحرب السبرانية. وثمة عقلية آخذة بالبروز تسمى «الحصار السبراني»⁽⁹³⁾.

مع ملاحظة أنّ ذلك المسرح الحربي هو جديد ومجهول، وكل ما يحدث فيه يجري بسرعة هائلة، وتذكّر ميل العسكر إلى التمسك بكونهم على حقّ دائماً؛ لأنهم يؤدّون مهمة ما، مهما كانت صيغتها؛ هرعت الجيوش كي تملأ ما بدا لها فراغاً آمناً. وترافق ذلك مع انتشار انطباع بأن هناك مشكلات عسكرية، وتبحث عن حلول عسكرية. وفي أسوأ الأحوال، تميل إلى التوتالية [الشمولية]، وتكون غير شرعية في أفضل الأحوال⁽⁹⁴⁾.

يجب إصلاح ذلك تماماً.

في الولايات المتحدة، هناك سلسلة من القوانين التي تحول دون تدخّل العسكر في الشؤون المدنية أيام السلم، مع ضمان جهوزيتهم للتصدي للتهديدات الخارجية. في العام 1878 ظهر «قانون بوزيه كوميتاتوس» (Posse Comitatus Act)⁽⁹⁵⁾، ثم تلتته تشريعات أخرى، لمنع العسكر من الانخراط في شؤون الأمن الداخلي. ولأننا قصرنا دور العسكر على الحرب ضد قوى خارجية، أنسنا إلى إعطائهم هوامش أكبر في الحركة. ومثلاً، لا تنطبق قوانين المصادرة والتفتيش المفروضة على قوى إنفاذ القانون على العسكر؛ لأنه ببساطة ليس منطقياً تطبيقها في غمار الحرب.

يجب أن تبقى العمليات العسكرية الهجومية في الفضاء السبراني تحت إشراف العسكر، سواء أكانت تجسّساً أم هجمات. في الولايات المتحدة، يترجم ذلك بـ «القيادة السبرانية الأميركية» (US Cyber Command)⁽⁹⁶⁾. إذا كنّا بصدد الهجوم على البنية التحتية الإلكترونية لبلد آخر، يجب التعامل مع ذلك كأى هجوم عسكري على بلد آخر. لا يتعلّق الأمر بالتجسس العادي (سواء في العالم السبراني أم الفعلي)،

بل بالهجوم. يجب النظر إلى تلك الهجمات السبرانية بوصفها أعمالاً عسكرية هجومية، ما يعني أيضاً وجوب إقرارها على أعلى مستويات السلطة التنفيذية، كما يجب خضوعها لمعايير القانون الدولي عينها التي تنطبق على الحرب الفعلية خارج الفضاء السبراني.

تقسيم «وكالة الأمن القومي»

بموجب الكلمات السابقة، اقترحت الفصل بين مهمتي الوكالة في التجسس والرقابة، وأن يقيّد دور العسكر في الفضاء السبراني بالأعمال التي تطال أهدافاً عسكرية أجنبية. ولإنجاز ذلك، أُويد تقسيم الوكالة مع تعزيز مسؤولياتها كافة التي كانت مناطة بها قبل 9/11:

* بوصفها جزءاً من وزارة الدفاع، يجب أن تبقى الوكالة تركيزها على التجسس على الحكومات الأجنبية.

* يجب أن تتولى وزارة العدل المسؤولية عن قوى إنفاذ القانون والتحقيقات المتصلة بالإرهاب. ولذا، يفترض أن يقتصر أمرها على الرقابة الموجهة والمجازة قانونياً، سواء أكانت داخلية أم خارجية؛ إضافة إلى توليها متابعة الأدلة المستندة إلى خبرات ضباط الـ «إف بي آي»، وليس قواعد البيانات في «وكالة الأمن القومي».

* يجب إبراز القدرات الدفاعية التي تمتلكها الوكالة في التشفير، وأمن الكمبيوتر، والدفاع عن الشبكات؛ مع جعلها علنية أكثر⁽⁹⁷⁾. يجب أن تُحكّم قبضة «المعهد الوطني للمعايير والتكنولوجيا» (National Institute of Standards & Technology) ويُعرف باسمه المختصر «نيست» (NIST)، هو وكالة مدنية تعمل خارج وزارة الدفاع على تطوير المعايير التقنية في أمن الشبكات. إذ حاول «قانون أمن الكمبيوتر - 1987»⁽⁹⁸⁾ إبقاء «وكالة الأمن القومي» خارج إطار الأمن المحلي بتوضيحه أن «نيست» - حينها، كان اسمها «المكتب القومي للمعايير» (National Bureau of

(Standards) تتولى القيادة في إرساء معايير الأمن التقني. نحتاج إلى تمتين ذلك القانون والتأكد من الالتزام به.

* يجب إبقاء القدرات الهجومية في الفضاء السبراني بيد «القيادة السبرانية الأميركية»، التي يجب أن تحوز القدرة على اختراق نُظُم الكمبيوتر التي تملكها «وكالة الأمن القومي»، (تسمى اختصاراً «تاو»). كذلك يجب ألا يتولى مدير الوكالة منصب القيادة في «القيادة السبرانية الأميركية».

من الواضح أنها خطة واسعة المدى، لكنها الخطة الصحيحة. وأثناء تنفيذها، يجب خفض تمويل «وكالة الأمن القومي» إلى المستوى الذي كانه قبل 9 / 11. من شأن ذلك بحد ذاته أن يترك آثاراً طيبة.

مكافحة الحركة باتجاه السيادة الوطنية في الفضاء السبراني

قبل عشرين عاماً، لم تحز سوى قلة من الدول قوانين تتحكم بالإنترنت. وحاضراً، تملك معظم الدول قوانين مشابهة، بل إن بعضها فائق القسوة. لا يبدو ذلك مفاجئاً لأن الإنترنت باتت شيئاً فائق الأهمية فلا تستطيع الحكومات تجاهلها. لكن بعض متابعي شؤون الإنترنت يدهشون من ذلك التحول، بل يقولون على دهشتهم أيضاً. باطّراد، تحارب حكومات عدّة الطبيعة العالمية المتأصلة في الإنترنت. إذا سعى حاكم لرقابة شعبه، والحدّ مما يستطيع قراءته، ولجم ما يقوله؛ عندها يمثل الطابع العالمي المفتوح للإنترنت مشكلة فعلية لذلك الحاكم.

وبسبب ذلك، ساندت حكومات كروسيا والصين والسعودية لسنوات طويلة فرض رقابة وطنية على الإنترنت ضمن تلك البلاد. وبواسطة مؤسسات دولية كـ «الاتحاد الدولي للاتصالات»، وهو مؤسسة تابعة للأمم المتحدة تتولى وضع معايير الاتصالات التليفونية؛ صارعت تلك البلدان ضد الإبقاء على الإنترنت بيد منظمات غير رسمية تملكها أطراف متعدّدة، وهو الوضع القائم حاضراً. تبدو

محاججات تلك الدول حميدة، لكن دوافعها ليست كذلك. إذ يريدون للإنترنت أن تقرّ بالحدود الوطنية، وبحق الحكومات في التحكم بها ضمن تلك الحدود أيضاً، ما يولّد مزيداً من الرقابة والحجب⁽⁹⁹⁾.

أعطى الكشف عن نشاطات «وكالة الأمن القومي» في الرقابة تدعيماً ضخماً لتلك المقاربة. قاومت حكومات كثيرة الهيمنة الأميركية على الإنترنت انطلاقاً من خشيتها على خصوصية مواطنيها. إذ دعت حكومات كالبرازيل⁽¹⁰⁰⁾ وألمانيا⁽¹⁰¹⁾ إلى تخزين معظم معلومات مواطنيها ضمن حدودها. وهناك حكومات لديها أجنداث معاكسة، لكنها تذرّعت بذلك الخطاب عينه. وسنّت روسيا قانوناً في 2014 يفرض على الشركات العاملة على الشبكة أن تخزّن معلومات مواطنيها ضمن حدود بلادهم، فتكون خارج متناول «وكالة الأمن القومي» لكنها طوع يد الحكومة الروسية⁽¹⁰²⁾.

لديّ آراء متضاربة في ذلك الشأن. فمن جهة، أرغب في رؤية قوانين قوية في حماية خصوصية المواطنين تعمّ الدول بطلب الأخيرة وضع المعلومات ضمن سلطاتها القانونية. ومن الجهة الثانية، لا أعتقد أن ذلك يحمي تلك البيانات من رقابة الوكالة. ففي الداخل الأمريكي، هناك على الأقل بعض من القيود على ما تستطيع الوكالة الوصول إليه. لكن، إذا خزّنت المعلومات في خوادم في ألمانيا والبرازيل، تزول تلك العوائق. ومع معرفة القدرات التقنية التي تحوزها الوكالة، لا يخامرني شكّ في أنها ستستطيع الوصول إلى تلك المعلومات على كل حال.

يعطي الطابع الدولي الأصيل في الإنترنت مغنم كثيرة للشعوب التي تعيش في بلدان يسودها الرقابة والحجب. غالباً ما تكون السيادة السبرانية مجرد ستار دخان يخفي رغبات السياسيين في رصد مواطنيهم ورقابتهم، من دون تدخّل شركات أو حكومات أجنبية. وكذلك ينظر إلى القتال ضد السيادة السبرانية بوصفها ستار دخان يخفي جهود «وكالة الأمن القومي» في كسب نفاذ أوسع إلى الاتصالات

العالمية. يجب علينا [الأميركيين] تجديد تمسكنا بدعم حرية الإنترنت وانفتاحها وعالميتها، ثم العمل على استمرارية وجودها بوصفها كذلك.

إعطاء الجمهور العام

تحوز الفضاءات العامة غير المملوكة فوائد اجتماعية جمّة. إذ لا تملك جهة خاصة أرفصتنا وطرقنا ومنتزهاتنا العامة، بل هناك قوانين تبين أنّ ملكيتها عامة. على الإنترنت، ترجع ملكية الأشياء كلها إلى جهات خاصة، حتى الموقع الخاص الذي يديره صديقك هو مستضاف على خوادم لشركة ما. لا ملكية للعامة.

ليس ذلك هو الانطباع الذي نملكه عن تجربتنا في استخدام الإنترنت⁽¹⁰³⁾. إذ تبدو الثروة عبر «فيسبوك» كأنها حديث شخصي، وتملكنا الدهشة عندما تمارس تلك الشركة حقوقها في حذف تدوينات ومنع أشخاص. وتزايد دهشتنا عندما نعلم أننا لا نملك الحق في مقاضاتها، بل ولا حتى في بياناتنا. نعم، لقد سلّمنا تلك الحقوق إلى الشركة عندما ضغطنا على زر الموافقة على الاتفاقية مع المستخدم. ولأننا لم نهتم بقراءتها فعلياً، لم نكن على معرفة كافية بها⁽¹⁰⁴⁾.

تكتسب الأمكنة العامة على الإنترنت أهميتها من واقع أن كثيراً من حرياتنا في العالم الفعلي تكون في أمكنة عامة. في الولايات المتحدة، يحمي التعديل الأول في الدستور حق التعبير في الأمكنة العامة. هناك قوانين أخرى تحظر نشاطات كالسكر والعردة في الأمكنة العامة. لا تنطبق تلك القوانين على الإنترنت لأن أمكنتها كلها تعود لملكيات خاصة⁽¹⁰⁵⁾. لا تنطبق تلك القوانين على ما نقوله في «فيسبوك» و«تويتر» و«إنستغرام» و«ميدوم» وغيرها⁽¹⁰⁶⁾، ولا على التعليقات التي ندونها في مواقع الأخبار، حتى لو كانت مفتوحة للقراءة من قبل العموم.

بالعودة إلى الأيام الأولى للإنترنت، كانت النقاشات تجري في منتديات عامة بواسطة ما سُمّي «يوزنت» (Usenet). مثلت «يوزنت» نظاماً غير مركزي لا يتيح

لأي شركة أن تحدّد من يقول ماذا. ومع انتقال منتديات النقاش إلى مواقع الـ«ويب» والمنصّات المملوكة من الشركات، تبخّرت تلك الحرّيّة.

نحتاج إلى أمكنة على الإنترنت لا تمتلكها أطراف خاصة، بل تكون أمكنة للحديث والحوار والتجمّع والاحتجاج. يمكن أن تكون أمكنة تديرها الحكومة، أو تديرها شركات خاصة تخضع لقوانين معيّنة تجعل من تلك المساحات عموميّة حقاً. وعلى غرار قوانين بث الموجات اللاسلكيّة التي تمنع شركات الاتصالات من التمييز بين أنواع الموجات المختلفة، من المتصوّر إمكان إيجاد شبكة اتّصال اجتماعي فيها مساحات عامة، ويديرها مُشغّل عمومي مع منع الشركات من الرقابة والحبس.

أيّاً كانت الحلول، يشكل الجمهور العام والمساحات العموميّة أمراً مهمّاً للمجتمع. يجب أن نعمل بدأب وتقصد لضمان حضورهم الدائم في الفضاء السبراني.

14

حلول للشركات

في خضم سعينا للحدّ من الرقابة التي تمارسها الشركات، من المهم تذكّر أننا نجني فوائد كبرى من تجميع المعلومات واستخدامها. إذ يمنحنا تجميع المعلومات فوائد وإمكانات غير مسبوقّة: الحصول على إرشادات لقيادة السيارة استناداً إلى معلومات جارية عن حال السير واختناقاته، قوائم مشتريات تتذكر ما اشتريناه في المرّة السابقة، إمكان الحصول على تعويضات على المشتريات حتى لو لم نحفظ بالفاتورة، إمكان التأكّد بواسطة الشبكة من إطفاء أنوار المنزل وإغلاق أبوابه، والتواصل فورياً مع الأشخاص في الأمكنة كافة على الكرة الأرضية. هناك مزيد من المنافع آتية. تكفي مشاهدة فيلم خيال علمي للتنبّه إلى الأعاجيب التي تحصل في عالم مؤتمت كلياً؛ خصوصاً إذا تأتت للحواسيب القدرة على فهم ما يفعله الناس والتجاوب معه وتذكّره أيضاً. يمثل ذلك النوع من الرقابة مستقبلنا الآتي، وهو مملوء بأشياء تجعل حياتنا أفضل وأكثر إمتاعاً.

على نحو مماثل، هنالك قيمة للوصول الحرّ إلى التكنولوجيا. وعلى الرغم من تركيز معظم هذا الكتاب على الجانب المظلم من التكنولوجيا، يجب علينا تذكّر أن التكنولوجيا أعطتنا جميعاً منافع جيّة. إذ تمكّننا التكنولوجيا من أداء أعمال معقّدة بسهولة وسرعة ودقّة ما يفيدنا في أشياء متنوّعة كتطوير مواد بناء أكثر ديمومة، العثور على المعلومات ونشرها، توقّع ظواهر فيزيائية معيّنة بدقّة كبيرة، التواصل

مع الآخرين مع التحرّر من قيود الجغرافيا، توثيق الحوادث الجارية، الحصول على طعام أكثر والعيش لمدة أطول. لم يكن بمكنتي إنجاز هذا الكتاب لولا الإنترنت. لا يعني ذلك أنه كامل بالطبع. وتتوزّع التكنولوجيا بشكل غير متعادل عبر الكرة الأرضية فيكون هنالك من يملكها ومن لا يملكها، لكن - بوجه عام - كلما زادت التكنولوجيا تكون الأشياء أفضل.

إنّ عرقلة المستقبل هو آخر ما نرغب في فعله. وببساطة، لا نعرف شيئاً عن المبتكرات الآتية، والمشاكل الإنسانية التي تستطيع حلها⁽¹⁾. نحتاج إلى امتلاك القدرة على التعامل مع التقنيات الجديدة ومع الأعمال التي تظهر استناداً إلى تلك التقنيات، بما فيها تقنيات الرقابة. وتمثّل المسألة في إيجاد توازن بين الوصول إلى الحدّ الأقصى من الفوائد المترتبة على تجميع الشركات للمعلومات من جهة، وتخفيض الأضرار الناجمة من ذلك إلى الحدّ الأقصى أيضاً.

ثمة حلول كثيرة تفيد في الوصول إلى ذلك الهدف. يشكل «إطار الخصوصية» الذي وضعته «منظمة التنمية والتعاون الاقتصادي» في 1980، نقطة انطلاق مناسبة؛ إذ يرسم حدوداً لعمليات جمع البيانات وتخزينها واستخدامها⁽²⁾. في 1995، أقرّ «قانون حماية المعلومات» في الاتحاد الأوروبي، بهدف تنظيم عمليات جمع البيانات الشخصية من قبل الشركات⁽³⁾. ولأن الشركات الأميركية تعودت على نظام تشريعي أقل صرامة في بلادها، فإنّها تبدي تبرّماً بذلك القانون الأوروبي⁽⁴⁾. ويجري نقاش واسع حاضراً عن تحديث ذلك القانون كي يتوافق مع التقنيات الحديثة⁽⁵⁾.

تتعلّق المقترحات المقدّمة في هذا الفصل بتجميع الشركات الخاصة للبيانات واستخدامها لها. أحياناً، من المحتمل أن يُطلّق السوق بنفسه بعضاً من تلك التغييرات، لكن معظمها يتطلّب قوانين تسهّل تنفيذه. إذاً، يبدو الأمر أشبه بقائمة

مما يجب على الحكومة القيام به، ما يعني أنها أيضاً قائمة بما يجب على المواطنون طلبه من الحكومة. ولأن مكونات تلك القائمة تمس الشركات، فإنها ترد في هذا الفصل.

لتتحمل الشركات مسؤولية اختراقات الخصوصية

يشكل تحميل الشركات مسؤولية اختراقات البيانات إحدى الطُرق الممكنة لتحسين أمن المعلومات المتجمعة لديها.

باستمرار، تعمل الشركات على الموازنة بين التكاليف والأرباح. في هذه الحال، تتمثل التكاليف في تكلفة تجميع البيانات وتخزينها، وما يتكلفه الاختراق وانعدام الأمان، وقيمة المعلومات المتجمعة. وحاضراً، لا يتكلف انعدام الأمان الشيء الكثير. إذا نحينا جانباً تكلفة الحفنة من الاختراقات العمومية - على غرار ما حدث مع شركة «تارغت»^(*)، تجد الشركات أنه من الأرخص إنفاق أموال على حملات دعاية تروج لجودة الأمن لديها، وتوهين الحملات التي تشور عرضياً في الصحافة مثبتة بطلان تلك المزاعم، وكذلك الحال بالنسبة للقضايا القانونية التي تحمل دلالة مماثلة؛ كما أنها لا تصلح الأمور إلا عندما تصل إلى مستوى العلانية.

"إطار الخصوصية" - "منظمة التنمية والتعاون الاقتصادي"
(1980)⁽⁶⁾

مبدأ تنظيم جمع المعلومات. يجب رسم حدود لعملية تجميع البيانات الشخصية، كما يجب الحصول على تلك المعلومات بطرق قانونية وعادلة، إضافة إلى إعلام المعني بها وموافقته، عندما يكون ذلك ملائماً.

مبدأ نوعية البيانات. يجب أن تتوافق البيانات الشخصية مع الأهداف التي تستعمل من أجلها، ويجب أن تكون دقيقة وكاملة ومحدثة، ضمن المدى الضروري لأهداف استعمالها.

مبدأ تعيين الغاية. يجب تعيين الهدف من جمع المعلومات الشخصية ضمن زمن لا يتأخر عن وقت تجميعها، مع مراعاة أن يجري استخدامها لاحقاً بما يتوافق مع تحقيق هذه الغايات أو غايات أخرى لا تكون متعارضة معها، ووفق ما يجري النص عليه في كل حال تشهد تغييراً في الغاية من استعمال تلك البيانات.

مبدأ تنظيم الاستخدام. يجب عدم الإفصاح عن البيانات الشخصية، أو جعلها متوافرة أو استعمالها بأي طريقة سوى تلك التي جرى تعيينها في الفقرة 9، ما عدا: أ) وجود موافقة من صاحبها؛ ب) بموجب سلطة القانون.

مبدأ ضمانات الأمن. يجب حماية المعلومات الشخصية بضمانات أمنية مناسبة تحميها من مخاطر تشمل الضياع والنفاد غير المشروع والتدمير والتعديل أو الانكشاف.

مبدأ الشفافية. يجب الالتزام بسياسة الشفافية العامة بصدد التطورات والممارسات والسياسات المتعلقة بالبيانات الشخصية. يجب أن تكون السُّبل متوافرة دوماً للتأكد من وجود البيانات الشخصية وطبيعتها، والغاية الرئيسة من استخدامها، إضافة إلى تحديد هوية المشرف على تلك البيانات ومكان إقامته.

مبدأ المشاركة الفردية. يجب أن ينال الأفراد الحق في: أ) الحصول من المشرف على البيانات أو من في حكمه، على تأكيد حيازته/ عدم حيازته بيانات تتعلق بهم؛ ب) أن يجري إبلاغهم بالبيانات المتصلة بهم. 1 - ضمن مدة معقولة 2 - بسعر لا يكون باهظاً، إن وُجد أصلاً 3 - بطريقة معقولة 4 - بشكل يكون مفهوماً لديهم؛ ت) الحصول على أسباب في حال عدم قبول تقدّمهم بطلب تحت البندين أ وب، مع إمكان أن يتحدثوا ذلك المنع؛

ج) أن يتحدّوا معلومات منسوبة إليهم، وفي حال نجاحهم بذلك، يفترض أن تمحى تلك المعلومات أو تعدّل أو تستكمل أو تصحّح.

مبدأ الموثوقية. يفترض بالمشرف على البيانات أن يكون موضع ثقة بالنسبة للاستجابة إلى الإجراءات التي تتعلّق بتفعيل المبادئ المنصوص عليها أعلاه.

يرجع السبب في ذلك إلى أن تكلفة اختراقات الخصوصية تقع على كاهل الجمهور الذي تنكشف بياناته. في علم الاقتصاد، يسمّى ذلك "خرجانية" بمعنى أن تأثير القرار لا يقع على عاتق متّخذه. وتحدّ "الخرجانيات" من حماسة الشركات لتحسين أمنها.

ربما تتوقّع أن يكون ردّ فعل الجمهور على ذلك هو تفضيل الخدمات المأمونة على غيرها؛ فبالنتيجة يتّخذ الجميع قرارات شرائهم بناءً لنموذج السوق نفسه. لكن، تذكّر أنّ ذلك ليس متاحاً عموماً. في بعض الأحيان، تحدّ بعض الاحتكارات في البرمجيات ما يتوافر من خيارات للجمهور. في حالات أخرى، يبرز تأثير "تناسب القفل مع المفتاح" الذي تتعمّده بعض الشركات التجارية البارزة في التكامل بين تركيبة الملفات، والبنية التحتية المتاحة، ومتطلّبات التوافق؛ أو بواسطة تقديم البرامج على هيئة خدمات؛ ما يصعب عملية الانتقال من خيار إلى آخر. في حالات كثيرة، لا نعرف من يجمع بياناتنا، كما ورد في النقاش عن الرقابة الخفية في الفصل 2. في الحالات جميعها، يصعب على الشّراء تقييم مدى مأمونية الخدمات. ولا يتعلّق الأمر بالشّراء غير التقنيّين، فحتى أنا لا أستطيع أن أفيدك عمّن تكل إليه خصوصيتك بثقة من بين مقدّمي الخدمات المختلفة.

يتغيّر ذلك مع تحميل الشركات المسؤولية القانونية للاختراقات. ومع رفع تكلفة اختراق الخصوصية⁽⁷⁾، نستطيع دفع الشركات للقبول بتكاليف «الخرجانية»، وإجبارهم على بذل جهد أكبر لحماية خصوصية أولئك الذين تجمّعت بياناتهم لديها.

في الولايات المتحدة، يحصل ذلك فعلياً مع بيانات الرعاية الصحية؛ لأن اختراق خصوصية البيانات فيها يترتب عليه غرامات باهظة⁽⁸⁾.

وكذلك شرع أمر مماثل في الحدوث أميركياً، في بيانات المتاجر أيضاً⁽⁹⁾. إذ تواجه «تارغت» حاضراً دعاوى قانونية ترتبت على اختراق البيانات لديها في العام 2013⁽¹⁰⁾. في حالات أخرى، جرت مقاضاة بنوك بسبب عدم وجود أمن مناسب لبيانات زبائنهم⁽¹¹⁾.

ربما تمثلت إحدى الطُرق التي تساعد على ذلك، في الطلب من الشركات بأن تبلغ المستخدمين عن كل المعلومات التي تملكها بشأن البيانات التي تعرّضت للضرر.

ربما تكون تلك الحالات معقدة، إذ تتضرر مجموعة من الشركات معاً في كل حادثة، ما يصعب التوزيع المناسب للمسؤوليات عليها⁽¹²⁾. وتلك المحاكم في تحديد قيمة معينة للخصوصية؛ لأن الناس تخلّوا طواعية عنها أصلاً مقابل الحصول على القليل. ولأنه من الصعوبة الربط بين الأضرار الناجمة من فقدان الخصوصية من جهة، والأفعال التي أدت إلى تلك الأضرار من الجهة الثانية، كان من الصعب كسب تلك الدعاوى.

هناك طريقة أفضل لمقاربة الأمر عينه: جعل القضية حدوث اختراق للخصوصية وليس ما ترتب على ذلك من أضرار. يجب إجبار الشركات على الانصياع إلى قوانين كـ «قانون الممارسات العادلة في المعلومات» (1973)⁽¹³⁾ وما يشبهه من قوانين لم تعد ملزمة حاضراً؛ وعندها يصبح الاعتداء هو الفشل في الالتزام بالقوانين.

"قانون الممارسات العادلة في المعلومات" (الولايات المتحدة - 1973)

يستند "قانون الممارسات العادلة في المعلومات" إلى 5 مبادئ:

1 - ألا يكون وجود نُظُم سجلات المعلومات الشخصية بحد ذاته سرياً.

- 2 - إيجاد طريقة كي يعرف المرء ما هي المعلومات المسجلة عنه، وكيف تستخدم.
- 3 - إيجاد طريقة يتمكن فيها المرء من منع وضع معلومات عنه جرى جمعها لغاية محدّدة في خدمة غايات أخرى إلا بموافقته.
- 4 - إيجاد طريقة تمكّن المرء من تعديل أو تصحيح سجل معلومات عنه، عندما تكون قابلة لأن تكون معروفة.
- 5 - على كل منظّمة تصنع أو تصون أو تستعمل أو تنشر سجلات فيها معلومات شخصيّة قابلة لأن تكون معروفة، أن تضمن مصداقية البيانات بالنسبة للغاية من استعمالها، كما يجب عليها اتخاذ احتياطات كافية لمنع سوء استعمال البيانات.

هنالك وضعيّة موازية تتمثل في قوانين "وكالة حماية البيئة" (Environment Protection Agency) بشأن ملوثات البيئة⁽¹⁴⁾. فعندما تتخطى الملوثات نسباً بعينها، تضحي عرضة للغرامات. لا حاجة لانتظار ظهور ارتفاع مفاجئ في حالات السرطان. تكون المسألة مفهومة، والقوانين مجهزة، ويكون على الشركات أن تقرّر بشأن بناء مصانع تعمل على الفحم أو الألواح الشمسيّة؛ وتكون العقوبات بالانتظار إذا فشلت الشركات في الانصياع إلى ما يمثل أفضل الممارسات بصورة أساسيّة. يجب أن نمضي في ذلك الطريق.

بالتأكيد، يؤول جعل النُظُم أكثر أماناً إلى زيادة التكاليف، وستسعى الشركات إلى إلقاء ذلك العبء على كاهل المستخدم بزيادة الأسعار، إذا تمكّنت من ذلك. لكن، بات المستخدمون يدفعون فعلياً تكلفة النُظُم غير الآمنة بالتكاليف المباشرة وغير المباشرة للاختراقات. تحميل الشركات المسؤولية القانونية عن الاختراقات، ينقل تلك التكلفة إليها ويؤدّي تالياً إلى دفعها لتحسين أمنها⁽¹⁵⁾. أفضل مصطلح

يعطيه علم الاقتصاد على ذلك هو «المتجنب بالكلفة الأقل»⁽¹⁶⁾، بمعنى أنه من المجدي اقتصادياً إلقاء المسؤولية على الطرف الذي يمتلك البيانات؛ لأنه في الوضع الأفضل لتقليص المخاطر إلى أقصى الحدود. فكّر في الأمر: ماذا تستطيع أن تفعل كي تجبر «فيسبوك» على تقديم حماية أفضل لبياناتك الشخصية؟ ليس كثيراً⁽¹⁷⁾. تفيد النظرية الاقتصادية أن ذلك يمثل سبباً لتحميل الشركة تكاليف ممارساتها السيئة في الأمن.

قوانين لاستعمال البيانات

خلافًا للحال في الاتحاد الأوروبي، لا تعتبر الولايات المتحدة أن المعلومات الشخصية هي ملك لك، بل تملكها الجهة التي تجمعها. تحمي القوانين أنواعاً معينة من المعلومات الشخصية - كالبيانات المالية، ومعلومات الرعاية الصحية، وبيانات الطلبة، وسجلات استئجار أشرطة الفيديو - لكن الأميركيين يفتقرون إلى قوانين عن الحماية الواسعة للخصوصية على غرار الحال في البلدان الأوروبية. في المقابل، تمثل الحماية القانونية الواسعة الحل الوحيد فعلياً؛ مع ملاحظة أن ترك الحبل على غاربه للسوق في تحديد ذلك سوف يؤدي إلى مزيد من الرقابة الواسعة العدوانية.

خذ هذا المثل: تعمل شركة «داتايوم» (Dataium) مع الأفراد أثناء شرائهم سيارات بواسطة الشبكة. وترصد زيارتك للمواقع الشبكية لمختلف صنّاع السيارات، فتلاحظ نوع السيارة التي تبحث عنها، الخيارات التي تنقر عليها لتعرف مزيداً من المعلومات عنها، الخيارات المالية التي تفتش عنها، وكم من الوقت تقضيه في مطالعة صفحات بعينها. يدفع المتعاملون أموالاً مقابل تلك المعلومات عنك، إذ إنها لا تتصل بالسيارات التي يبيعونها، بل بالسيارات التي صنعتها شركات أخرى ولفتت اهتمامك كثيراً⁽¹⁸⁾. ويدفعون مقابل تلك المعلومات لأنك إذا قصدت معارضهم، يصبحون أكثر قدرة على بيع سيارة لك بما يضمن ربحاً أكثر لهم.

عند هذه النقطة، فكّر في الاقتصاديات. بإمكان تلك المعلومات أن تكلفك (بأدنى تقدير) قرابة 300 دولار من السعر النهائي الذي تدفعه لشراء سيارتك.

يعني ذلك أن حمايتك من ممارسات «داتايوم» لا تساوي أكثر من 300 دولار. لكن، هنالك 12 مليون سيارة تباع سنوياً في الولايات المتحدة. حتى لو افترضت أن «داتايوم» تملك بيانات تتصل بـ2 في المئة منهم، فإن ذلك يعني أن التكتيكات التي تتبعها تلك الشركة تساوي 100 مليون دولار سنوياً.

يشكل ذلك التفاوت السبب في فشل الحلول الآتية من السوق. إنها مسألة عمل جماعي. إذًا، عملنا المشترك في حماية أنفسنا من ممارسات «داتايوم» يساوي 100 مليون دولار، لكننا لا ننسق أعمالنا معاً. وتربط «داتايوم» بين وكلاء السيارات بصورة طبيعية، لكن الوسيلة الوحيدة للربط بيننا كمستهلكين هو الفعل السياسي.

إنّ نقاط الاستعمال هي مكان منطقي لفرض قوانين تنظيمية؛ لأن كثيراً من البيانات التي تُجمَع عنا يجري تحصيلها عندما نكون راغبين في ذلك. ونحتج عندما تستعمل البيانات بطرق لم نكن نقصدها: عندما نخزن ونشارك ونُباع ونُستق، ثم نستخدم للتلاعب بنا بطرق خفية. يعني ذلك وجود حاجة لقيود على الطرق الممكنة في استخدام بياناتنا، خصوصاً تقييد تلك الطُرق التي تغيّر الأهداف التي جمعت تلك البيانات لأجلها.

تثور مسائل أخرى عندما تعامل الشركات جداول خوارزمياتها بوصفها أسراراً تجارية. هناك مثلاً على ذلك هما: جدول خوارزمية «بايج رانك» (Page Rank) في «غوغل» الذي يحدّد نتائج البحث التي تعرض عليك، ونُظُم تسجيل بيانات بطاقات الائتمان. تملك الشركات هاجساً شرعياً بالسرية. ونخشى وصول المنافسين إلى خوارزمياتها وبياناتها (مع قدرتهم على نسخها)، قدر خشيتها من وصول الجمهور إليها وانكشاف طرق عملها أمامه. وشخصياً، أرى أن الشفافية تتقدّم على الملكيات التجارية في الأحوال التي تطاول الخوارزميات فيها الجمهور

بتأثيراتها⁽¹⁹⁾. من المستطاع جعل المزيد من الخوارزميات علنية - بل تصميمها لتكون قابلة للعلانية - بالمقارنة مع ما يحصل حاضراً⁽²⁰⁾. لسنوات طويلة، فرضت الصراحة في القروض وقوانين العدل فيها أن تكون الخوارزميات التي تستخدمها المؤسسات المالية، قابلة للشرح والمساءلة القانونية. يجب مدّ أطر تلك الشفافية المفروضة إلى مساحات أخرى تمارس فيها الخوارزميات سلطتها على الناس؛ بمعنى جعلها مفتوحة. وفي المقابل، هنالك طُرُق في تدقيق الخوارزميات تضمن عدالتها مع الحيلولة دون انكشافها للعلن⁽²¹⁾.

تميل الشركات لأن تكون منطقية في تقييم المخاطر، وستتقيد بالقوانين. إن المفتاح الحقيقي لنجاح ذلك الأمر هو الإشراف والموثوقية. ليست تلك أشياء استثنائية، فهنالك قوانين كثيرة تنظم صناعات أميركية عدّة؛ لأننا نعرف أن ما يفعلونه هو مهم وخطير في آن معاً. وليس من فارق بين ذلك وبين المعلومات الشخصية وخوارزميات تحليلها.

يجب إرساء آلية للتدقيق تضمن التزام الشركات بالقوانين، وتعاقبها إن لم تفعل ذلك.

يبدو ذلك كله منطقياً من الناحية النظرية، لكن تنفيذه صعب. الحال أن آخر ما نرغب به هو أن تبدأ الحكومة بالقول: «يمكنكم أن تفعلوا ذلك حصراً، لا سواه»، بالنسبة لبياناتنا ومعلوماتنا. إذ تتكفل القوانين التنظيمية المستندة إلى الأذن الحكومي المسبق، بخنق التغيير والابتكار التقني. إننا نسعى إلى قوانين تنظيمية مستندة إلى الحقوق أساساً، فيكون شعارها: «تستطيع فعل ما تشاء، طالما أنه ليس محظوراً».

تنظيم جمع المعلومات أيضاً

لا يكفي تنظيم استخدام البيانات. إذ يجب تنظيم الخصوصية في مسارات كثيرة تشمل جمع البيانات وتخزينها واستعمالها، وكذلك الخلافات بصددّها. ويظهر إطار

الخصوصية» في «منظمة التنمية والتعاون الاقتصادي» (1980) تلك الأشياء بطريقة حسنة، وهي أساسية كلها. ولسنوات طويلة، بذلت الشركات الأميركية جهوداً منسقة لإقناع العالم بعدم الحاجة إلى قوانين لتنظيم جمع المعلومات، والاكتفاء بقوانين استخدامها⁽²²⁾. تسعى الشركات إلى التخلص من القيود على جمع البيانات؛ لأنها تعلم أن القيود على استعمال البيانات ستكون صعبة التحديد وضيقة المدى، وأنها [الشركات] تستطيع توسيعها تدريجياً ما أن تصبح بياناتنا في أيديها. (ثمة حجة رائجة ضد كل قانون لتنظيم استخدام البيانات تتمثل في وصمه بأنه شكل من الرقابة). وتعلم الشركات أنه بمجرد وضع قوانين لتنظيم جمع البيانات، يصبح من الصعب تغييرها. ولكن، على غرار الرقابة الحكومية العامة، يلحق الضرر بالخصوصية من محض تجميع البيانات، وليس حصراً من استعمالها⁽²³⁾. أذكر بالنقاش عن الرقابة بالخوارزميات في الفصل 10. سوف ينجم عن عدم تنظيم جمع المعلومات إلى تجميع واسع لها، ومشاركة مفرطة للبيانات مع الحكومة، مع تآكل بطيء للقيود الضرورية المحددة بدقة على استخدام البيانات.

يجدر بنا القتال ضد تلك الحملة. ليست القيود على جمع المعلومات أمراً مستحدثاً. إذ لا يطلب من الموظفين المعنيين أن يسألوا المتقدمات إلى وظيفة ما عما إذا كنَّ حوامل. لا يسمح لاستمارات طلب القروض البنكية أن تتضمن سؤالاً عن عرق المتقدم بالطلب. مثلت التسوية القديمة بشأن عدم طلب الإفصاح عن الهوية الجنسية بالنسبة للجنود مثليي الجنس في الجيش الأمريكي، وهي التي لخصها شعار «لا تسأل، لا تُخبر»، قيلاً على جمع المعلومات. وهناك قيود على ما يستطيع «المكتب الأمريكي للإحصاء» أن يسأل الناس عنه.

لن يكون من السهل نقل تلك الأمور إلى عالم يتحكم فيه الكمبيوتر بكل ما نفعله، لكن يجب أن نبدأ بالنقاش عن المعلومات التي يجب عدم السؤال عنها أبداً. ثمة أمكنة واضحة للانطلاق منها. يجب أن يكون ما نقرؤه على الشبكة الإلكترونية يمثل خصوصية ما نقرؤه ورقياً. ويعني ذلك ضرورة وضع حدٍّ قانوني للسجلات

عن الصفحات الشبكية التي قرأناها، والوصلات الإلكترونية التي نقرنا عليها، ونتائج عمليات البحث التي أجريناها على الإنترنت. ينطبق الأمر نفسه على تحركاتنا، بمعنى ضرورة التخلص من حال يكون فيه اقتناء الخلوي رديفاً للوقوع في آسار رقابة مستمرة. يجب التوقف عن الرصد المستمر لعلاقتنا، بمعنى مع من نلتقي في الشارع ومن نتحدث إليهم. لربما سُمح لشركات بأن تستخدم بعضاً من بياناتنا فوراً، شريطة أن تتخلص منها. ولربما سُمح لشركات بالاحتفاظ ببياناتنا لبعض الوقت، شريطة ألا يطول.

هناك فكرة جذابة طرحها البروفسور ميخائيل فرومكين، وهو أستاذ في كلية القانون بجامعة ميامي⁽²⁴⁾. تتمثل الفكرة في إلزام الوكالات الحكومية والشركات الخاصة، لدن انخراطها في عمليات واسعة لجمع المعلومات، بأن توقع «تعهداً بشأن تأثير الخصوصية» يكون على شاكلة «تقارير الأثر البيئي». إذ يفيد ذلك في إعلام الجمهور عما يُجمع من بيانات مع تبيان سبب جمعها. وسوف يبحث ذلك صُناع القرار على التفكير في الخصوصية في مرحلة مبكرة من تطوير مشاريعهم، مع التماس آراء الناس بصددھا.

يصلح خيار الدخول كنقطة انطلاق. وبشكل أساسي، هناك طريقتان للحصول على موافقة. يعني خيار الدخول اشتراط الحصول على موافقتك الصريحة قبل جمع بياناتك واستخدامها. يعني خيار الخروج نقيض ذلك تماماً، بمعنى أن بياناتك ستُجمع إلا إذا اخترت الاحتجاج صراحة على ذلك. تميل شركات كـ «فيسبوك» إلى تبني خيار الخروج؛ لأنها [الشركات] تستطيع جعل العثور على ذلك الخيار صعباً، كما أنها تعلم أن معظم الناس لا يبالون بالأمر. يبدو خيار الدخول أشد عدلاً بكثير، كما يجب عدم جعل استخدام الخدمة مشروطاً بالموافقة على جمع البيانات والمعلومات.

حتى الآن، لا جانب مظلم لجمع البيانات وتخزينها كلها. ومع تقييد ما تستطيع الشركات جمعه من المعلومات وما تستطيع فعله بها، ومع جعل الشركات مسؤولة عن البيانات المتجمعة لديها، ومع إرغامها على النزاهة التامة مع الجمهور بشأن ما تجمعه حقاً وكيف تتصرف به؛ نصل إلى وضع نؤثر فيه في الشركات كي يقتصر ما تجمعه وتخزنه من بيانات عنا، على ما تعرف الشركات أن له قيمة حقاً.

يجب على الكونغرس أن يخطر في عمل دؤوب لتحديث قوانين الخصوصية في الولايات المتحدة، والتوقف عن إعطاء الذرائع لتعاضده. تستطيع المحاكم أيضاً أن تؤدي دوراً مهماً في ضمان خصوصية المستهلك، بتفعيل القوانين السارية بشأن الخصوصية. تحوز بعض الوكالات التشريعية، كـ «اللجنة الفيدرالية للتجارة» و«اللجنة الفيدرالية للاتصالات»، بعض السلطة في حماية خصوصية المستهلك في مجالات معينة⁽²⁵⁾. في المقابل، تحتاج الولايات المتحدة حاضراً إلى وجود وكالة مستقلة لحماية المعلومات، أسوة بما هو حاصل في بلدان كثيرة⁽²⁶⁾. ونحتاج إلى ما هو أفضل من المسارعة إلى سدّ المشكلات عندما ينتج عنها ضرر كافٍ. إنها تحديات كبيرة ومعقدة، وتحتاج إلى وجود وكالة تملك خبرة ومصادر كافية للتأثير فيها بشكل مجدٍ.

إنجاز العمل ببيانات أقل

إلى حد كبير تماماً، تستطيع المؤسسات إنجاز أعمالها مع تجميع بيانات أقل كثيراً مما تفعله الآن، وتخزينها لفترات أقصر أيضاً. المفتاح اللازم لذلك هو أن تفهم [الشركات] كمية البيانات التي تحتاجها، وتحدّد الغاية منها.

مثلاً، تعمل نُظُم كثيرة على تجميع هويات المستخدمين دون حاجتها إلى تلك المعلومات. وغالباً، يكون التفويض هو كل ما تسعى إليه. لا يحتاج موقع للتواصل الاجتماعي إلى معرفة هويتك الحقيقية. وكذلك الحال بالنسبة الشركة التي تعمل على تخزين البيانات في «سُحُب المعلومات».

ثمة أنواع من تحليل البيانات تتطلب الحصول على بيانات عن أشخاص كثيرين، لكن ليس كل شخص. لننظر إلى تجربة شركة «وايز» (Waze). إنها تستخدم معلومات الرقابة لتتبع أوضاع حركة السير، لكنها لا تحتاج إلى معلومات عن كل شخص كي تنجز عملها. إذا وضعت تحت الرقابة عدداً من السيارات يكفي لتغطية الشوارع الرئيسية، فسيكون ذلك كافياً. وتعتمد مجموعة من محلات البيع بالتجزئة على الرقابة الشاملة لقياس فعالية إعلاناتها، واستنتاج أنماط الشراء عند الجمهور وغيرها. كرة أخرى، لا تحتاج تلك المحلات إلى بيانات الناس كلها. إذ تكفي عينة إحصائية جيدة الدلالة لتلك التطبيقات، وهو أمر كان رائجاً عندما كان جمع المعلومات مكلفاً.

هنالك تطبيقات تميل لتجميع بيانات عن الجميع كي تزيد فعاليتها، ببساطة⁽²⁷⁾. لكن، من المؤكد أن «غوغل» سيعمل جيداً إذا امتلك بيانات عن نصف جمهور مستخدميه، لكنها ستكون تجارة أقل ربحاً. يبقى أن ثمة تطبيقات تحتاج البيانات كلها. إذا كنت شركة للخلوي تسعى إلى إيصال المكالمات الهاتفية، فستحتاج إلى معرفة موقع كل مستخدم، وإلا سينهار النظام بأكمله.

ثمة تفاوتات بين الشركات في مدة تخزين البيانات. تحتاج «وايز» والشركة التي تقدّم لك خدمات الخلوي إلى معرفة موقعك باستمرار، في الوقت الحي. يحتاج المعلنون إلى بعض البيانات المتسلسلة زمنياً، لكن المعلومات الأكثر جدّة تكون أشد أهمية لهم. من الناحية الثانية، هناك بيانات فائقة القيمة للبحوث. ومثلاً، تضخ شركة «تويتر» بياناتها إلى «مكتبة الكونغرس»⁽²⁸⁾.

نحتاج إلى قوانين ترغم الشركات على جمع الحد الأدنى اللازم من البيانات، والاحتفاظ بها لأقل زمن لازم، مع حفظها بطريقة أكثر أمناً مما تفعله [الشركات] الآن. وكما يبدو متوقعاً، تملك اللغة الألمانية كلمة واحدة لوصف ذلك كله هي «داتنشابارشمز امكايت» (Datensparsamkeit)، وهي تعني «اقتصاد البيانات»⁽²⁹⁾.

إعطاء الناس الحق في بياناتها

الولايات المتحدة هي البلد الغربي الوحيد الذي لا يملك قوانين لحماية البيانات⁽³⁰⁾. تملك أميركا حمايات لبعض أنواع المعلومات، لكنها تشمل حقولاً معزولة⁽³¹⁾. بصورة عامة، فإنّ حقوق الأميركيين في بياناتهم تتسم بالتشوش. و«يتذكّر» محرّك البحث «غوغل» معلومات عن حياتي، نسيبتها أنا منذ زمن طويل⁽³²⁾. يرجع ذلك لا متلاك «غوغل» سجلاً عن عمليات البحث التي أجريتها طيلة حياتي، لكنني لا أملك نفاذاً إليها كي أنعش ذاكرتي. تزعم شركة «ميدترونيك» أن المعلومات الموجودة في أجهزتها لإنعاش القلب بالصدمة الكهربائية، هي ملكية تجارية لها، ولا تتيح للمرضى الذين جاءت من قلوبهم تلك البيانات الحق في الوصول إليها⁽³³⁾. في الاتحاد الأوروبي، يملك الناس الحق في معرفة المعلومات والبيانات المتعلقة بهم. ولذا، استطاع الشاب ماكس شريمز إرغام شركة «فيسبوك» على إعطائه البيانات المتعلقة به لديها كافة^(*). لا يتمتع المواطنون الأميركيون بذلك الحق.

لا يسهل تصوّر الطريقة التي يجب تفعيل تلك الحقوق بها. مثلاً، يمكن إيراد قائمة عن أنواع البيانات التي نتجها بأنفسنا على شبكات الـ «سوشال ميديا»⁽³⁴⁾:

✱ بيانات الخدمة: إنها البيانات التي تعطيها للشبكة الاجتماعية كي تحصل عليها. ووفقاً لكل موقع، يحتل أن تشمل تلك البيانات اسمك القانوني وعمرك ورقم بطاقتك الائتمانية.

✱ بيانات مُعلّنة: هي التدوينات التي تخطّها على صفحتك، بما فيها مواد المدوّنة الإلكترونية، والصور وأشرطة الفيديو والرسائل والتعليقات وغيرها.

(*) راجع الفصل 1 في الكتاب.

✱ البيانات الموثوقة: إنها ما تكتبه على صفحات الآخرين. وتشبه أساساً البيانات المعلنة، ويكمن الفارق في أنك لا تحظى بالسيطرة عليها، بل إن المستخدم الآخر هو الذي يحظى بها.

✱ البيانات العرضية: هي ما يكتبه آخرون عنك. ربما كانت فقرة تتحدث عنك في شيء كتبه شخص ما، أو ظهورك في صورة التقطها شخص آخر ووضعها على الإنترنت. لا يقتصر الأمر على أنك لا تسيطر على تلك البيانات، بل إنك لم تصنعها أصلاً.

✱ البيانات السلوكية: إنها البيانات التي يجمعها الموقع عن عاداتك، بمراقبته ما تفعله والأشخاص الذين تتعامل معهم.

✱ بيانات مشتقة: هي معلومات عنك تُستخلص من البيانات الأخرى كافة. مثلاً، إذا عرّف 80 ٪ من أصدقائك أنفسهم بوصفهم مثلي الجنس، فالأرجح أنك مثلي الجنس أيضاً.

ما هي الحقوق التي تملكها في أنواع تلك البيانات كلها؟ في الوضع الحاضر، كل تلك البيانات موضوعة على الطاولة. هناك أنواع من البيانات تحتفظ بخصوصيتها دوماً، بعضها يمكن جعله خصوصياً، وبعضها يبقى عمومياً دوماً. من المستطاع تعديل بعض البيانات أو حذفها - شخصياً، أعرف موقعاً يسمح بحذف البيانات الموثوقة بصورة نهائية خلال 24 ساعة - ويستعصي بعضها على ذلك. يمكن الاطلاع على بعض البيانات، ولا يسمح بذلك بالنسبة لبيانات أخرى. لا قوانين في الولايات المتحدة عن البيانات، ويجب على من يملكون البيانات أن يقرّروا بأنفسهم، وهم بالتأكيد يحظون بنفاذ كامل لها.

تقدّم لك بعض المنصّات إمكانات مختلفة في تقييد من يطلع على بيانات اتصالاتك. ووصولاً إلى العام 2011، كان «فيسبوك» يتيح لك إمكان تقييد من يطلعون على تدويناتك، بمعنى اقتصار ذلك على أصدقائك أو إتاحتها للعموم. وعند تلك النقطة من الزمن، كان «فيسبوك» يسمح لك بالتحكّم بمجموعة

أصدقائك، وبأن تطلع بعضاً منهم على تدويناتك، وليس كلهم بالضرورة⁽³⁵⁾. تنقسم التغريدات إلى ما يوجّه إلى أشخاص بعينهم، وما يعلن على الملأ⁽³⁶⁾. من المتاح جعل تدوينات «إنستغرام» سرّية، أو مقلّودة من أشخاص بعينهم، أو معلنة للعموم⁽³⁷⁾. وتمنح صفحات موقع «بينترست» إمكان جعلها معلنة أو سرّية⁽³⁸⁾.

من المهم وضع معايير لتلك الأمور. في العام 2012، أصدر «البيت الأبيض» ما يعرف باسم «وثيقة حقوق الخصوصية للمستهلك». في 2014، أوصت لجنة مراجعة رئاسية عن الخصوصية و«البيانات الضخمة»، بجعل تلك الوثيقة أساساً في التشريع⁽³⁹⁾. أوافق على ذلك تماماً.

من السهل المضي بعيداً في ذلك المفهوم. يقترح يارون لانير، عالم كومبيوتر وناقد للتقنية، خطة تقضي بأن نحصل تلقائياً على جُعالةٍ من كل من يستخدم بياناتنا، سواء أكان محرّك بحث يستعملها لإيصال إعلانات إلينا أم تطبيقاً رقمياً يستعملها لتحديد درجة اختناق المرور⁽⁴⁰⁾. بالطبع، ستكون جُعالة ميكروسكوبية، أو ربما نانوية؛ لكنها ربما تراكمت لتصل إلى حفنة من الدولارات. يتّسم تنفيذ تلك الخطة بالتعقيد الفائق، وبالنتيجة يحتاج التنفيذ إلى رقابة مستمرة حتى لو أنه يسعى إلى تحويل الرقابة إلى مصدر مالي لكل شخص. تتمثل المسألة الأساسية في تبني مفهوم الخصوصية بوصفها شيئاً قابلاً للتجارة بتلك الطريقة. لكن الخصوصية يلزمها أن تكون حقاً أساسياً، وليس ملكية تجارية.

"وثيقة حقوق الخصوصية للمستهلك" - الولايات المتحدة (2012)⁽⁴¹⁾

التحكّم الفردي. يحقّ للمستهلكين ممارسة التحكّم بالبيانات الشخصية كافة التي تجمعها الشركات منهم، وكذلك طُرُق استعمال تلك البيانات.

الشفافية. يحقّ للمستهلكين الحصول على معلومات بخصوص ممارسات الأمن والخصوصية تكون سهلة الفهم والوصول.

احترام السياق. يحقّ للمستهلكين توقع أن تجمع الشركات بياناتهم الشخصية وتستخدمها وتكشفها بطرق تتناسب مع السياق الذي أعطى فيه المستهلكون تلك البيانات.

النفاذ والدقة. يحقّ للمستهلكين الوصول إلى بياناتهم الشخصية وتصحيحها في الملفات قيد الاستخدام، بطريقة تتناسب مع حساسية البيانات والمخاطر المتنوعة التي قد تنجم إذا لم تكن البيانات صحيحة.

الموثوقية. يحقّ للمستهلكين أن تكون بياناتهم الشخصية بيد شركات تتقيد بإجراءات مناسبة لضمان توافقها مع «وثيقة حقوق الخصوصية للمستهلك».

يجب أن نمتلك الحق في الحذف. يجب أن نكون قادرين على القول لكل شركة أوكلنا إليها بياناتنا: "نحن نغادرك. نرجو حذف البيانات المتعلقة بنا كافة". يجب أن تكون قادراً على القول لسماسة المعلومات والبيانات: "لست منتجاً بيدك. أنا لم أعطك أبداً الإذن بجمع معلومات عني وبيعها للآخرين. أريد إخراج بياناتي من قاعدة بياناتك". يحاول الاتحاد الأوروبي التعامل مع ذلك الأمر: الحق في النسيان⁽⁴²⁾. في العام 2014، قضت «محكمة العدل الأوروبية» بأنه في بعض الأحيان، يجب على محرّكات البحث أن تحذف معلومات عن أفراد من نتائج عمليات البحث فيها⁽⁴³⁾. أدى ذلك إلى تدفق سيول من الناس على «غوغل» طالبن حذف نتائج بحث لا تعبّر عنهم بدقة؛ وشملت صفوف هؤلاء سياسيين وأطباء والمثاليين جنسياً إلى الأطفال⁽⁴⁴⁾. من المستطاع إثارة نقاش عن خصوصيات تلك الحال، وإذا كانت المحكمة توصلت إلى التوازن الصحيح، لكن يبقى أن ذلك حق مهم للمواطنين في بياناتهم التي تستفيد الشركات منها⁽⁴⁵⁾.

إبراز الخصوصية وجمع البيانات

طيلة الوقت، نُبرز بيانات عن أنفسنا إلى العائلة والأصدقاء والزملاء والمحبين، بل حتى الغرباء. نشارك معلومات مع أطبائنا ومستشارينا الماليين وأطبائنا النفسيين.

نتشارك معلومات كثيرة. لكننا نفكر بتلك المشاركة على طريقة المعاملات: أنا أشارك معك بيانات لأنني أريد أن أطلعك على أشياء، أو لأنني أؤمنك على أسراري، أو أنني أتعامل معك بالمثل لأنك أطلعتني تَوّاً على شيء ما خصوصي بشأنك.

لقد طوّر الجنس البشري نظماً سيكولوجية من الأنواع كافة، لاجتياز تلك المفازة من القرارات بشأن الخصوصية. وتتميز تلك النُظم بأنها معقدة بشكل استثنائي، عالية التناغم، وحساسة اجتماعياً. تدخل إلى حفلة ما فتعرف فوراً كيف يجب أن تتصرّف. تعرف لمن تتحدث، ما الذي تقوله لمن، من يقترب منك ومن يصغي إليك؛ يستطيع معظمنا اجتياز تلك التجربة بصورة طيبة. ثمة مشكلة في كون التقنية تثبّت تلك القدرة الاجتماعية. انقل مشهدية تلك الحفلة إلى «فيسبوك»، يبدأ حدسك في الحوار فجأة. إذ ننسى من يقرأ تدويناتنا. وعلى نحو عرضي، ربما وضعنا شيئاً خصوصياً في متناول العلن. لا نفهم كيفية ترصد بياناتنا في خلفية الموقع. لا ندرك ما تستطيعه التقنيات التي نستعملها، وما الذي تعجز عنه.

وإلى حدّ كبير، يرجع ذلك إلى عدم إبراز درجة الخصوصية على شبكة الإنترنت. يتواهن الحدس عندما تتوارى أفكار الخصوصية في خلفية المشهد. عندما لا نقدر على فهم الناس، يحقق بنا الفشل. إذ لا نفكر بشيء من قبيل «هناك شركة تسعى إلى الربح تسجّل كل شيء وتسعى إلى تحويل ذلك إلى إعلانات». لا نفكر بأنّ «الولايات المتحدة وربما حكومات أخرى تسجّل كل ما أقوله، وتبحث عن الإرهابيين أو المجرمين أو مهرّبي المخدرات أو كل شخص سيئ اختارته هذا الشهر». ليس ذلك ما يبدو واضحاً في مشهدية الإنترنت. إنّ ما يبدو واضحاً هو «أنا جزء من هذه الحفلة الافتراضية، مع أصدقائي وزملائي، ونحن نتحدث عن أمور شخصية».

لذا، ليس بالمستطاع استخدام إظهار الناس المستمر لبياناتهم الشخصية على تلك المواقع، بوصفه دليلاً لموافقتهم على وضعهم تحت المراقبة. ما يوافق الناس عليه هو أن الإنترنت فيها موازاة للعالم الفعلي الذي تحتزن رؤوسهم معرفتهم به، ولا

يفهمون على نحو كامل الشعبات والإملاءات كافة من انتقال ذلك العالم الحقيقي إلى الفضاء السبراني⁽⁴⁶⁾.

تفضّل شركات كـ «فيسبوك» أن تجري الأمور على ذلك النحو. وتخرج [الشركات] عن طُرُقها المعتادة كي تتأكّد من أنّك لا تفكّر بالخصوصيّة أثناء وجودك على مواقعها، كما تستخدم خدعاً معرفيّة لزيادة ثقتك بها، كأن تعرض عليك صور أصدقائك. تذهب الحكومات أبعد من ذلك بجعلها معظم رقابتها سرّية، فلا يعرف الناس شيئاً عما يحدث. يعطي ذلك تفسيراً للانفصال بين دعاوى الناس بأهمية الخصوصية من جهة، واستمرارهم في أفعال تدلّ على العكس؛ ذلك أنّ النُظم التي نستعملها مصمّمة كي لا تبرز قضية الخصوصية⁽⁴⁷⁾.

هناك حاجة لإعطاء الناس خيار الخصوصية الحق على الإنترنت، والقدرة على فهم ذلك الخيار وتبنيه. ستضحي الشركات أقلّ ميلاً لفعل أشياء مريبة ببياناتنا، في حال يجب عليها أن تبرّر نفسها أمام مستخدميها ومستهلكيها⁽⁴⁸⁾. وسيصبح المستعملون أقلّ إغواءً بدعاوى «المجاني»، إذا عرفوا التكاليف الحقيقيّة⁽⁴⁹⁾. سوف يقتضي ذلك فرض قوانين عن «الحقيقة في المنتج» لتنظيم عمل الشركات، إضافة إلى قوانين مماثلة لتنظيم عمل الحكومة.

في البدايات، سيجب على المواقع الشبكيّة الكشف عما تسعى إليه الأطراف الثلاثة أثناء تتبع زوّار تلك المواقع، ويجب على شركات الهواتف الذكيّة أن تكشف عن المعلومات التي تسجّلها عن مستخدميها. هناك أمكنة كثيرة تُمارَس فيها الرقابة خفية، ويجب جعلها بارزة أيضاً.

مرّة أخرى، ذلك أمر صعب. إذ تشكّل المعرفة والخيار والموافقة طريقة صحيحة للتعامل مع ذلك الوضع⁽⁵⁰⁾، لكننا نعرف لا جدوى تلك الصيغة من سياسات الخصوصية المصاغة بلغة قانونيّة مقعّرة؛ وهي التي نوافق عليها عندما نضغط زر «أوافق» على ما يعرض علينا. وعند سابق قصد، جُعِلَت تلك الصيغ طويلة

وتفصيلية، وبالتالي مملة ومُربكة؛ كما أنها لا تنتج موافقة مجدية من قبل المستخدم. لا يراودنا شك أيضاً في لا جدوى ظهور تلك النافذة التي تقفز على الشبكة في كل مرة ندون فيها شيئاً ما على «فيسبوك»، لتقول: «ما كتبته سيخزن في «فيسبوك» ويستخدم للتسويق، كما يعطى إلى الحكومة عندما تطلبه». نحتاج إلى حلّ وسط. ويرادوني ظنّ بأنّه يشمل وضع سياسات معيارية ونوع من الشهادة أو الإجازة لكل طرف ثالث.

إرساء مرجعيات موثوقة للمعلومات

في مناح كثيرة من حيواتنا، نمح المختصين نفاذاً إلى معلومات شخصية جداً عن أنفسنا. وكما نثبت من كونهم لا يستعملونها إلا لمصلحتنا، جرى إرساء مفهوم مسؤولية المرجعية. يتقيد الأطباء والمحامون والمحاسبون بقوانين تطلب منهم وضع مصلحة زبائنهم فوق مصالحهم الخاصة. تتحكم تلك القوانين بكيفية استخدامهم المعلومات والسلطة المخولة إليهم، ولا تتيح لهم عموماً استعمال المعلومات لأهداف غير ذات صلة. هناك قوانين تفرض على الشرطة متى يستطيع طلب معلومات من المرجعيات الموثوقة. تخلق علاقة المرجعية الموثوقة واجب الاهتمام الذي يتقدم الالتزامات الأخرى كافة.

نحتاج إلى مرجعيات موثوقة في المعلومات⁽⁵¹⁾. الفكرة وراء ذلك أنهم سيصبحون شريحة مؤسساتية تمسك بالمعلومات، وتكون عرضة لقيود وحمايات قانونية خاصة. يجب على الشركات أن تقرر إذا ما كانت ستنضوي في تلك الشريحة أم لا. يتشابه ذلك مع المستشارين الاستشاريين الذين يملكون مسؤولية المرجعية، فيما لا يملكها الساسرة⁽⁵²⁾. وبهدف تحفيز الشركات على التحول إلى مرجعيات موثوقة، تستطيع الحكومات منح إعفاءات ضريبية وحمايات قانونية للشركات التي تقبل تلك المسؤولية المضافة. ربما نُظِرَ إلى بعض أنواع الأعمال بوصفه مرجعية موثوقة بصورة تلقائية، ببساطة بسبب الكميات الكبيرة من المعلومات الشخصية التي تجمعها بصورة طبيعية. يشمل ذلك مقدّمي خدمات الإنترنت، شركات

الخلوي، مقدمي خدمات البريد الإلكتروني، محرّكات البحث ومنصّات التواصل الاجتماعي.

من شأن تنظيم المرجعيّات إعطاء الناس الثقة بأنّ معلوماتهم لا تسلّم إلى الحكومة، أو تباع إلى طرف ثالث، أو تستخدم ضدّهم. كما يمحض حمايات خاصة للمعلومات الموكولة إلى المرجعيّات الموثوقة. ومن شأنه أيضاً أن يفرض واجبات معينة في الرعاية على من يدير المعلومات، كأن يكون مستوى معيّناً من الأمن، والتعرّض للتدقيق بصورة منتظمة وما إلى ذلك. يكفل ذلك التنظيم تفعيل الثقة.

ويخطوط مشابهة، اقترح خبير أمن الإنترنت دان غير أن يختار مقدّمو خدمات الإنترنت بين كونهم شركات محتوى أو شركات اتّصالات⁽⁵³⁾. فبوصفهم شركات محتوى، يستطيعون استعمال البيانات والاستفادة منها، كما يتحمّلون مسؤولية قانونيّة عنها. وبوصفهم شركات اتّصالات، لا يترتب عليهم مسؤولية حيال المعلومات، لكنهم لا يستطيعون قراءتها.

في العصور الوسطى، فرضت الكنيسة الكاثوليكيّة واجباً صارماً من السريّة حيال الذنوب التي يجري الاعتراف بها، معتبرة أن أحداً لن يشارك في طقس الأسرار الإلهيّة إذا خشي الناس خيانة الكاهن للأسرار التي يأتمنونه عليها. نحتاج حالياً إلى ثقة من ذلك النوع على الإنترنت.

تحفيز نماذج عمل جديدة

صارت الرقابة نموذج العمل على الإنترنت لأنها شكّلت أسهل الطرق في الحصول على المال، مع غياب قوانين تنظّمها⁽⁵⁴⁾. واستمرت نموذجاً للعمل على الإنترنت بأثر من انخفاض التكاليف، وضخامة الأرباح المتوخاة، و(أقله في الولايات المتّحدة) استمرار غياب قوانين تنظّمها.

وبوضع قوانين تنظّم جمع البيانات واستعمالها معاً، ورفع تكلفة الاحتفاظ بالبيانات، سنحفّز بصورة طبيعية نماذج جديدة في العمل لا تكون مستندة إلى الرقابة. وتتوافر القدرات التقنية لإنجاز ذلك. هناك بحوث عدّة عن إرساء الخصوصية في المنتجات والخدمات من البداية، بمعنى آخر يتعلق الأمر بثبيت الخصوصية في تصاميمها⁽⁵⁵⁾. إذ يجب ألا تتبّع شركات بطاقات الائتمان تفاصيل مشترياتنا كافة، كي تصنع فواتيرها وتتجنّب الفساد. يجب على مقدمي خدمات الخلوي ألا يحتفظوا بسجلات أبدية عن مواقعنا كي يستمروا في تقديم المكالمات والرسائل النصية. من المستطاع بناء إنترنت تتضمن حمايات قويّة لمغفلي الهوية. يمكن للنقود الإلكترونية أن تكون آمنة وبلا هوية. تلك الأشياء كلها ممكنة، لكن يجب أن نطالب بها.

يجدر الإقرار بأن الآلية المطلوبة ستكون بطيئة. إذ تعتقد الشركات الأكثر توسّعاً في جمع بياناتنا بأن فيها إمكانات كامنة لمداخيل ضخمة تأتي من الإعلانات. ربما يصل حجم سوق إعلانات الإنترنت إلى قرابة 125 بليون دولار عالمياً، لكنه يمثل ربع القيمة الإجمالية لسوق الإعلانات. تضع شركات كـ «فيسبوك» و«غوغل» نصب أعينها الأموال التي تنفق على إعلانات التلفزة (40٪ من إجمالي السوق) والصحف والمجلات (36٪)⁽⁵⁶⁾. كذلك وظّفت شركات الإنترنت أموالاً طائلة في «البيانات الضخمة» التي تعني جمع البيانات كافة ثم التفكير في أوجه التعامل معها لاحقاً، ولن تبدّل توجهاتها بسهولة. يطلق الصحافي جايمس كانستلر على ذلك «سيكولوجية الاستثمار السابق»⁽⁵⁷⁾، وهو السبب عينه الذي يجعلنا نضّيع أموالاً بعد أن نكون قد تصرفنا جيّداً بالأموال التي سبقتها. من الصعوبة الإقرار بأنك على خطأ، خصوصاً أن تكلفة جمع البيانات وتخزينها منخفضة تماماً.

في اقتصاد السوق، إذا لم تتمكن شركة ما من وضع نموذج عمل مربح، سيتقدّم الذين نجحوا في ذلك. إذا نجحنا في رفع تكلفة الرقابة وجمع المعلومات، ستظهر أنواع من الأعمال لا تستند إليهما [الرقابة وجمع المعلومات]، كما تحل بديلاً للأنواع الموجودة حاضراً وهي تعتمد عليهما.

لنقاوم رقابة الحكومة

حتى الآن، تمثلت النتيجة الأهم لكشوفات سنودن في أنها حطمت الشراكة بين الحكومة والشركات في الرقابة، وهي التي بيّنتها في الفصل 6. قبل سنودن، لم يكن هنالك ضير في تعاون شركة ما مع «وكالة الأمن القومي». إذا طلبت الوكالة إمدادها بنسخ عن كل الحركة الإلكترونية على الإنترنت، أو زرعت «أبواباً خلفية» في منتج يفترض أنه يحمي أمن البرامج، كان من المستطاع افتراض أن ذلك التعاون سيقى سرّاً إلى الأبد. وإنصافاً، لم يتعاون الجميع طواعية مع الوكالة. قاوم بعضهم في المحاكم⁽⁵⁸⁾. في المقابل، يبدو أن الغالبية التي ضمت صفوفها خصوصاً شركات الاتصالات الاحتكارية التي تهيمن عليها الدولة والشركات العملاقة للإنترنت، رحّبت بإعطاء الوكالة نفاذاً غير مراقب لكل ما طلبته. كان ذلك سهلاً، وفعله الجميع أثناء الحرب الباردة ثم عقب هجمات 9/11، بلا ضوضاء.

أخذ ذلك المشهد بالتغيّر. إذ باتت هناك قيمة للانحياز إلى الخصوصية ومقارعة «وكالة الأمن القومي»، إضافة إلى حدوث ضرر من التعاون معها. هناك أربعة طرق رئيسة تسلكها الشركات في مقاومة الوكالة، هي: الشفافية، والتقنية، والتقاضي، ومجموعات الضغط.

تلجأ مجموعة من شركات الكمبيوتر، كـ «مايكروسوفت» و«ياهو» و«غوغل» وغيرها، إلى نشر «تقارير شفافية» دورياً، تعطي فكرة عامة عن عدد طلبات البيانات التي تلقتها الشركات من الحكومة، وكم مرّة استجابت لها⁽⁵⁹⁾. من الواضح أن العلاقات العامة هي المحرك الأساسي لنشر التقارير، بمعنى القول للجمهور إن نسبة صغيرة من بياناته تقدّم للحكومة. ومثلاً، في العام 2013، زعمت شركة «غوغل» أنها سلّمت إلى الحكومة الأميركية «بيانات وصفية» عن اتصالات الإنترنت تشمل ما يتراوح بين 1 و2000 مستخدم، إضافة إلى محتويات الاتصالات لما يتراوح بين 18 ألفاً و20 ألف مستخدم⁽⁶⁰⁾. هناك قوانين تحكم تلك

الأرقام لأنه من غير المسموح للشركات أن تعطي الأرقام الدقيقة، على الرغم من أن بعضها يضغط على الحكومة كي تسمح بإعلان أرقام أكثر دقة. (تقدّم تقارير «غوغل» أرقاماً أكثر دقة عن الطلبات من حكومات أخرى، غير الولايات المتحدة).

وعمدت حتى شركات الاتصالات والكابل الأميركية إلى نشر تقارير شفافية، بداية من التقرير الذي أصدرته شركة «كريدو موبايل» (CREDO Mobile) للاتصالات، في مطلع العام 2014⁽⁶¹⁾. تملك تلك التقارير قيمة أقل من سواها. مثلاً، أورد تقرير من شركة «فريزون» للاتصالات أنها تلقت قرابة 320 ألف طلب للحصول على البيانات، من قبل «قوى إنفاذ القانون» في العام 2013⁽⁶²⁾. نعلم أنه كل 3 شهور تتلقّى «فريزون» رسالة واحدة من «وكالة الأمن القومي»، تفرض عليها تسليم «البيانات الوصفية» لزبائنها كافة الذين يقدر عددهم بـ 290 مليوناً⁽⁶³⁾، فما معنى الـ 320 ألفاً؟

تحاول بعض الشركات السير إلى أبعد من ذلك. في 2014، أعلنت شركة «آبل» أنها ستعلم كل مستخدم فرد بشأن طلب الحكومة بياناته، إلا إذا منعتها الحكومة من ذلك بصورة محدّدة إفرادياً⁽⁶⁴⁾. وشكّلت «مايكروسوفت» و«غوغل» حلفاً قانونياً لمقاضاة الحكومة والحصول على مزيد من الشفافية⁽⁶⁵⁾. وسارت «ياهو» في المسار عينه⁽⁶⁶⁾.

هناك شركات توظّف أشخاصاً كي يبلغوها سرّاً عن صدور مذكرات قضائية تأمرها بعدم الإفصاح عن تسليم بياناتها إلى جهات رسمية، ويسمّى هؤلاء «عصافير المذكرات»⁽⁶⁷⁾. ومنذ 2013، تتضمن تقارير الشفافية من شركة «آبل» العبارة التالية: «لم تلق «آبل» إطلاقاً أمراً تحت الفصل 215 من «قانون باتريوت» في الولايات المتحدة». وتنقل العبارة فكرة مفادها أنّه لو تلقت «آبل» ذلك الأمر، لما سُمح لها بالإفصاح عن تلقيها إياه، لكن إزالة تلك العبارة تحمل إشارة إلى المتابعين

اليقظين. لم تحسم المحاكم أبداً بشأن قانونية تلك الممارسة، وشخصياً أبدي تشككي في نجاعتها، لكنها تمثل جهداً شجاعاً وذكياً⁽⁶⁸⁾.

على الجبهة التقنية، ترفع شركات عدة وتيرة استعمالها للتشفير في اتصالاتها مع زبائنها ومستخدميها بواسطة الإنترنت، وفي شبكاتنا الداخلية، وفي قواعد بياناتها⁽⁶⁹⁾. بعد أن علم «غوغل» أن «وكالة الأمن القومي» تنصّت على الجسم الأساسي للروابط الإلكترونية في الاتصالات بين قواعد بياناتها؛ عمد إلى تشفير تلك الروابط⁽⁷⁰⁾. وبعد أن علم «ياهو» أن الوكالة تنصّت على الصلات الشبكية بين مستخدميه ومواقع «ياهو»⁽⁷¹⁾، شرع في تشفيرها بالتعاون مع «مايكروسوفت»⁽⁷²⁾، التي افترضت أن أمراً مماثلاً يحدث مع مستخدميها ومواقعها⁽⁷³⁾. وأخذت شركات كبرى في خدمات البريد الإلكتروني بتشفير ذلك البريد أثناء تنقله بين قواعد بياناتها⁽⁷⁴⁾. تبذل شركات أخرى جهوداً أكبر في تشفير الاتصالات التي تربطها بزبائننا ومستخدميها⁽⁷⁵⁾. اعتمدت هواتف الـ «آي فون» والـ «آندرويد» التشفير كإجراء أساسي⁽⁷⁶⁾. بات «غوغل» يقدم خيار التشفير بين طرفي التراسل بواسطة بريد «جي ميل»، على الرغم من حدسي بأن ذلك الخيار لن يروج كثيراً؛ لأن المستخدمين لن يتمكنوا من البحث في رسائلهم وتصنيفها، إذا بقيت مشفرة⁽⁷⁷⁾.

في المحاكم، يجب على الشركات أن تترافع لمصلحة جمهور مستخدميها. يجب أن تطلب مذكرات من المحاكم لكل عملية وصول إلى بياناتها، وأن تقاوم قضائياً في حال تلقيها مذكرات تتوسّع في النفاذ إلى بياناتها بشكل مفرط. يحدث بعض من ذلك منذ مدة. في العام 2008، حارب «ياهو» سرّاً «وكالة الأمن القومي» في المحاكم، وعاند لفترة طويلة قبل أن ينضم إلى برنامج «بريزم»^(*) في الوكالة⁽⁷⁸⁾. في 2012، أخفق «تويتر» في معركته ضد طلب حكومي بتسليمها معلومات تتصل بنشاط

في حركة «احتلوا وول ستريت»⁽⁷⁹⁾. في 2014، خاض «فيسبوك» معركة قضائية ضد مدعي عام مقاطعة نيويورك الذي طلب تسليم رسائل خاصة وصور ومواد مُشابهة؛ لاستعمالها في بحث جنائي عن فساد في مؤسسة «الضمان الاجتماعي»⁽⁸⁰⁾.

بوسع الشركات أن تفعل أكثر من ذلك لدعم جهود التقاضي. إذ يجب أن تحتفظ بملخصات قضائية عن آراء الخبراء الذين تستشيرهم المحاكم قانونياً بشأن قضايا ربما شكّلت سوابق قضائية تمسّ تلك الشركات. في 2013، طلب الـ «إف بي آي» المفتاح الشامل للملفات مستخدمى البريد الإلكتروني كافة لشركة «لافايت»، بهدف الوصول إلى بريد أحد المستخدمين. لم ترفع أي من الشركات الكبرى للبريد الإلكتروني، كـ «غوغل» و«مايكروسوفت» و«ياهو» وغيرها، دعاوى قضائية بشأن ذلك التصرف⁽⁸¹⁾. لم تفعل؟ يجب على الشركات أن تدرك أن ذلك الشأن يطالنا جميعاً.

مرة أخرى، يشكّل الطابع الدولي للإنترنت ثنية معقّدة في ذلك المجال. من المستطاع أن تختار شركة ما الانصياع إلى الطلبات القانونية للبيانات في بلدها، فهاذا عن بقية البلدان؟ في أربع مناسبات في السنوات القليلة التي تلت العام 2000، انصاع محرّك البحث «ياهو» لطلب من الحكومة الصينية بيانات عن أفراد من مستخدميهم، استُخدِمت في توقيفهم وسجنهم بتهمة «التخريب» و«كشف أسرار الدولة»⁽⁸²⁾. هل يجب على «ياهو» الانصياع؟ هل من فارق إذا كان نظام قمعي ما (...) على علاقة طيبة مع الولايات المتحدة؟ تزعم مجموعة من شركات الإنترنت أنها لا تكون تحت سلطة البلدان التي لا مكاتب لها فيها. ربما لا تستطيع شركة أمريكية أن تقاوم القانون الصيني، لكنها تستطيع مقاومة بلدان أخرى أصغر وأقل قوّة. بطرق كثيرة، تستطيع تلك الشركات أن تختار أي البلدان تطيع القانون فيها، وأيّها لا تفعل ذلك. يجب عليها أن تختار تعظيم خصوصيّة مستخدميها إلى أقصى حدّ.

في الأروقة السياسية، يجب على الشركات أن تستعمل نفوذها السياسي. إذ تنخرط شركات كـ «مايكروسوفت» و«فيسبوك» و«غوغل» وغيرها، بنشاط مع مجموعات الضغط السياسي، بهدف فرض قيود قانونية على ممارسة الحكومة الأميركية للرقابة⁽⁸³⁾. إنه أمر جيد، لكن هناك حاجة إلى مزيد منه. في أغلب الأحيان، تأتي الحجج السياسية الأكثر إقناعاً من شركات مهتمة بالوصول إلى خلاصات الأمور.

كذلك يجب عدم الإفراط في ذلك كله. إذ إن مصالح الشركات ربما تقاطعت مرحلياً مع مصالح الخصوصية لدى المستخدمين، لكنهما ليسا متحالفين دائماً. لسنوات طويلة، قاتلت الشركات ضد القوانين التي تحدّ من قدرتها على جمع البيانات واستخدامها. بذل الاتحاد الأوروبي جهوداً من أجل إقرار تشريعات أكثر صرامة وحدائث في ذلك الشأن، لكنه جوبه بحملات ضارية من مجموعات الضغط التي تعمل لمصلحة شركات الإنترنت الأميركية غير الراغبة في التوقف عن جمع المعلومات⁽⁸⁴⁾. إن هذه الهيكلية الصاعدة حاضراً في الوقوف بوجه «وكالة الأمن القومي»، هي أقرب لكونها حملة لتغيير رؤية المستخدم، من كونها جهوداً تهدف لإيجاد حلّ لمشكلة الخصوصية. لذا، نحتاج أيضاً إلى قوانين قوية تضبط الشركات أيضاً.

نحو وثيقة «ماغنا كارتا» جديدة

دعا المهندس الإلكتروني السير تيم بيرنرز لي، وهو مبتكر «الشبكة العنكبوتية الدولية»، إلى صوغ وثيقة «ماغنا كارتا» (Magna Carta)^(*) جديدة تعمل على تقييد الحكومات والشركات معاً⁽⁸⁵⁾، وتفرض مسؤوليات على الشركات التي تعمل في عصر المعلوماتية، فلا تكتفي بالحقوق وحدها⁽⁸⁶⁾. وعملياً، ليست تلك المقارنة

(*) في العام 1215، أرغم بارونات إنكلترا الملك جون الأول على توقيع وثيقة الـ «ماغنا كارتا» (ترجمتها حرفياً: «الشرعة العظيمة») التي تضمن الحريات الأساسية في المجتمع. وتعدّ الوثيقة صيغة تأسيسية أولى للديمقراطية في الغرب.

التاريخية عظيمة، لكن تلك الفكرة العامة جديرة بأن تكتشف. وتمثل أيضاً الفكرة الأساسية التي أدعو لها في هذا الكتاب.

هل تذكر أنني في الفصل 4، وصفتُ العلاقة بين الشركات والمستخدم بأنها إقطاعية؟ يرجع ذلك لكونها علاقة مُغرِضة وأحادية الجانب. إذ تتأسس على اتفاقية للمستخدم النهائي جرت صياغتها بصيغة قانونية مربكة للعقل، كما تستطيع الشركة تغييرها وفق رغباتها. تاريخياً، كانت الإقطاعية شبيهة بذلك، بمعنى أن اللوردات امتلكوا الحقوق كافة، فيما لم يفرض عليهم سوى النزر اليسير من المسؤوليات. في أوروبا القرون الوسطى، أدى صعود الدولة المركزية وحكم القانون، إلى إعطاء الإقطاع المرونة التي كان يفتقدها. وفي 1215، صارت الـ «ماغنا كارتا» أول وثيقة حديثة تصون وتحتضن فكرة أن شرعية الحاكم تأتي من أتباعه، وأخضعت الملك لحكم القانون. في البداية، ألزمت الوثيقة الملوك بمسؤوليات حيال اللوردات التابعين لهم، ثم توسعت تدريجياً لتضع المجتمع على طريق حكم الشعب بالشعب وللشعب.

في القرن الثامن عشر، عندما شرعت الدول في إدراك أن سلطتهم في الحكم تنبع من الشعب كله، سادت الفلسفة السياسية للمفكر الإنكليزي توماس هوبز، الذي دافع عن فكرة تضحية الشعب بالسلطة والحرية ليضعهما بيد متسيد مطبوع على الخير يكون واجباً عليه إعطاء الشعب خدمات متنوعة، بما فيها الأمن⁽⁸⁷⁾. وحاجج الفيلسوف الإنكليزي جون لوك ضد تلك الفكرة واصفاً تلك الصيغة من العلاقة بين المتسيد والشعب بأنها غير عادلة وغير متوازنة، معتبراً أن الحكومات تستمد سلطاتها من «موافقة المحكومين»⁽⁸⁸⁾. أشعلت مفاهيم لوك الثورات في إنكلترا وفرنسا وأميركا، وأدت إلى صوغ «إعلان حقوق الإنسان والمواطن» في فرنسا، و«وثيقة الحقوق» في الولايات المتحدة.

"إعلان مدريد للخصوصية" (2009) (89)

يغتتم المجتمع المدني فرصة اللقاء السنوي 31 لـ "المؤتمر الدولي لمفوضي الخصوصية وحماية البيانات" كي:

- 1 - يحدّد الدعم لإيجاد إطار عن «الممارسات العادلة في المعلومات» يفرض واجبات على أولئك الذين يجمعون المعلومات الشخصية ويتعاملون معها، ويعطي حقوقاً لمن تُجمعت معلوماتهم الشخصية.
- 2 - يحدّد الدعم لإيجاد سلطات مستقلة لحماية البيانات، تتخذ قراراتها ضمن إطار شرعي، بشفافية ومن دون مصلحة تجارية أو تأثير سياسي.
- 3 - يحدّد الدعم لإيجاد تقنيات لتمكين الخصوصية، يكون من شأنها تقليص أو إنهاء عمليات جمع معلومات معرّفة بأنها شخصية، وكذلك وضع تقييمات لتأثير الخصوصية بطريقة مجدية تفرض الانصياع لمعايير الخصوصية.
- 4 - يحضّر البلدان التي لم تقرر «ميثاق مجلس أوروبا 108» مع «بروتوكول 2001» أن تفعل ذلك بأسرع وقت ممكن.
- 5 - يحضّر البلدان التي لم ترسّ إطاراً شاملاً لحماية الخصوصية وسلطة مستقلة لحماية البيانات أن تفعل ذلك بأسرع وقت ممكن.
- 6 - يحضّر البلدان التي أرسّت أطراً قانونية لحماية الخصوصية أن تضمن التنفيذ الفعال وتدعمه، وأن تتعاون على المستويين الدولي والإقليمي.
- 7 - يحضّر البلدان على التثبت من إشعار الأفراد بسرعة عندما تتعرض معلوماتهم الشخصية للانكشاف غير المناسب، أو للاستعمال بطريقة لا تتلاءم مع تجميعها.
- 8 - يوصي ببحوث شاملة عن مدى مواءمة تقنيات إخفاء هوية البيانات، للتثبت من كونها عملياً تمثل طرقاً تحمي الخصوصية وإغفال الهوية.

- 9 - يدعو إلى وقف تطوير أو تنفيذ نُظُم جديدة في الرقابة العامة، بما فيها التعرّف إلى الوجه، والتصوير المسحي للجسم كاملاً، المعرّفات البيولوجيّة، واللواحق المغنطة بطريقة «ريفد»؛ مع وضعها قيد تقييم شامل وشفاف من قِبَل سلطات مستقّلة، وبنقاش ديمقراطي.
- 10 - يدعو إلى تأسيس إطار دولي جديد لحماية الخصوصية، مع المشاركة الكاملة للمجتمع المدني، يكون مستنداً إلى حكم القانون، واحترام الحقوق الأساسيّة للإنسان، ودعم المؤسسات الديمقراطية.

في كتابها بعنوان موافقة المتصلين بالشبكات، أثارت الصحافيّة والمدافعة عن الحقوق الرقمية ريبيكا ماكينون، النقطة التالية: «لن تكون أي شركة مثاليّة، ولن يوجد متسيّد مثالي، مهما حسّنت النوايا والفضائل عند الملك أو الملكة أو الديكتاتور المطبوع على الخير. وتلك هي النقطة تماماً، بمعنى أن عقدنا الاجتماعي مع العواهل الرقميّين تجري على مستوى بدائي، وهوبزي [نسبة للمفكر هوبز] وملكيّ. إذا كنّا معظوظين، يكون العاهل جيّداً ونصليّ كي لا يكون ابنه أو خليفته المختار شيطاناً. هناك سبب لكون معظم الناس لم يعد يقبل بذلك النوع من التسيّد. حان الوقت كي نرتقي بالعقد الاجتماعي المتعلّق بالحوكمة الرقمية لحيواتنا إلى المستوى الذي دعا المفكّر لوك إليه. ويعني ذلك أنّ إدارة هويّاتنا ودرجة وصولنا إلى المعلومات، يمكنها أن تعبّر بأصالة وإخلاص عن موافقة المتصلين بالشبكات»⁽⁹⁰⁾.

تتمثّل الفكرة في أنّ صوغ «ماغنا كارتا» جديدة تكون أشد تركيزاً على المؤسسات التي أساءت استعمال السلطة في القرن 21، سيكون لها تأثير يشابه نظيرتها التاريخيّة. هناك بعض الوثائق اقتربت من تلك الفكرة. إذ ما زال «إعلان مدريد للخصوصيّة» (2009) يعدّ الصيغة الأشد تماسكاً لحقوق الخصوصية في العصر الحديث.

15

حلول للبقية منا

تمثل الرقابة مشكلة قانونية وتقنية. وغالباً، تصل الحلول التقنية إلى يد المستخدم. نستطيع استعمال تقنيات للخصوصية وإغفال الهوية لحماية بياناتنا وهوياتنا. تتسم تلك التقنيات بالفعالية، لكن يمكن خنقها بواسطة أوامر حكومية سرية. ويجب أن نخوض معركة سياسية في ذلك أيضاً.

تتطلب الحلول السياسية جهداً جماعياً، لكنها غالباً تجري ضمن بلدان محددة. وتميل الحلول التقنية إلى العالمية. إذا صممت «مايكروسوفت» نظام تشغيلها «ويندوز» وزودته بتشفير شامل، وإذا قرّر «فريق العمل على هندسة الإنترنت»^(*) (Internet Engineering Task Force) أن كل ما يمر في الإنترنت يجب أن يشفر، تطل تلك المتغيرات كل شخص في العالم عند استخدامه تلك المنتجات والبروتوكولات. إذاً، المسألة هي أن السياسة بإمكانها تخريب التقنية، كما تستطيع التقنية أن تخرب السياسة. لا يتقدم أحدهما على الآخر. إذا سعينا للإصلاح، يجب علينا القتال على جبهتي السياسة والتقنية معاً. ولا يتصل ذلك بالحكومات والشركات. هناك الكثير مما نستطيع نحن الشعب أن نفعله.

(*) هي هيئة دولية من مهندسي الإنترنت وتقنييها ومشغليها وباحثاتها تعنى بتطوير هندسة تلك الشبكة. وتأسست في 1986، وهي مفتوحة أمام الجمهور.

مقاومة الرقابة

كتب أستاذ القانون البروفسور آيبن موغلين: «إذا لم نرتكب أخطاءً، يكون لدينا الحق في فعل كل ما بوسعنا للحفاظ على التوازن التقليدي بيننا وبين السلطة المنتصّة. نملك الحق في أن نكون غامضين. نملك الحق في الغمضة. نملك الحق في التحدّث بلغات لا تفهمها الحكومة. ونملك الحق في أن نلتقي في الزمان والمكان الذي يناسبنا»⁽¹⁾. إذا جلس رجل بوليس ضمن مدى السمع ليتنصّت علينا، يكون من حقنا الانتقال إلى مكان آخر. إذا تمترس قرب بيتك ضباط الـ «إف بي آي» في شاحنة تعجّ بالكاميرات، فمن حقك تماماً أن تسدل الستائر والحُجُب.

وعلى غرار ذلك، هناك طُرُق متنوّعة تمكّننا من حماية بياناتنا بأنفسنا، وأن ندافع عن أنفسنا ضد الرقابة. وسأصنّف تلك الطُرُق ضمن مجموعات مستقلة⁽²⁾.

تجنّب الرقابة. تستطيع أن تغيّر عاداتك كي تتجنّب الرقابة. تستطيع أن تدفع نقداً لشراء بعض الأشياء بدلاً من استعمال بطاقة الائتمان، أو أن تتعمّد تغيير طريقك لتجنّب كاميرات مراقبة المرور. تستطيع التوقّف عن إنشاء صفحات على «فيسبوك» لأطفالك، وتمتنع عن وضع تعريفات على صورهم المنشورة على الشبكة. تستطيع التوقّف عن استخدام «مفكرة غوغل» وأنوع البريد الإلكتروني المستند إلى الـ «ويب»، إضافة إلى تجنّب تخزين المعلومات في «السحب الرقمية». تستطيع استعمال محرّك البحث «داك داك غو» في التفتيش عن المعلومات على الإنترنت. تستطيع ترك هاتفك الخلوي في المنزل، وهي طريقة سهلة لتجنّب التتبع. بتحديد أكثر، تستطيع ترك هاتفك الخلوي وحاسوبك عندما تسافر إلى بلدان كالصين وروسيا، وتكفي باستخدام معدّات مستأجرة.

تستطيع تجنّب التشغيل الأوتوماتيكي لنُظُم الرقابة بتعمّدك عدم تشغيل خوارج ميات التتبع لتلك النُظُم. مثلاً، تستطيع إبقاء تعاملاتك المالية النقدية تحت الحدّ الذي يُطلَب فيه من المؤسسات المالية تبليغ الحكومة عنه. بإمكانك أن تنأى

بنفسك عن نقاش مواضيع معينة عبر البريد الإلكتروني. في الصين، تسود الرقابة الأوتوماتيكية ما يضطر الناس أحياناً إلى كتابة رسائل على الورق، ثم إرسال صور عن تلك الرسائل بواسطة البريد الإلكتروني. لا ينفع ذلك الإجراء في مواجهة الرقابة الموجهة، لكنه يصعب الأمور على الرقابة الأوتوماتيكية. وتعمل تقنية الـ «ستغانوغرافيا» (Steganography)، ومعناها كتابة معلومات سرّاً ضمن رسائل أو صور عادية-، ضمن أفق مشابه.

صدّ الرقابة. يشكّل ذلك الطريق الأكثر أهمية لحماية أنفسنا. ربما تملك «وكالة الأمن القومي» ميزانية تفوق مجموع ما يرصد لوكالات التجسس كافة لدول العالم بأسره، لكن ذلك لا يجعلها سحراً، وكذلك الحال بالنسبة لبقية وكالات التجسس في البلدان كلها. يعتمد التجسس الفعال على الاقتصاد والفيزياء والرياضيات. وتستطيع الوكالات الأمنية في العالم كله هزيمتك إذا ركزت عليك بشخصك، إلا أن الرقابة العامة تعتمد على الوصول السهل لبياناتنا ومعلوماتنا. ويتمكن الدفاع الجيد إرغام من يسعون إلى رقابتنا على انتقاء أهدافهم؛ لأنهم ببساطة لا يملكون موارد كافية لاستهداف كل شخص على حدة.

هنالك ما يسمّى «تقنيات تعزيز الخصوصية» (Privacy Enhancing Technologies) ⁽³⁾ ويشار إليها بالاسم المختصر «بت» (PET)، تستطيع أن تساعدك في صدّ الرقابة العامة. هناك تقنيات كثيرة تساعدك في حماية بياناتك. ثمة مكونات رقمية أساسية للاتصال بالإنترنت، يمكن إدخالها في محركات البحث بهدف تقصي المواقع التي تتعقبك أثناء تجوالك على الإنترنت وصدّها، وهي تشمل «لايت بيم» (Lightbeam) و«برايفسي بادرجر» (Privacy Badger) ⁽⁴⁾ و«دسكوننكت» (Disconnect) و«غوستري» (Ghistry) و«فلاش بلوك» (Flash Block) وغيرها ⁽⁵⁾. تذكر أن خيارات خصوصية التجوّل الموجودة في متصفحك تتولّى حذف البيانات موضعياً ⁽⁶⁾. ويعني ذلك أنها تفيد في إخفاء زيارتك للمواقع الإباحية عن أعين زوجتك، لكنها لا تصدّ عمليات ملاحقتك على الإنترنت.

التقنية الأكثر أهمية بين أنواع الـ «بت» هي التشفير. ويعطيك برنامج «بيت لوكر» (Bit Locker) الذي تصنعه «مايكروسوفت»⁽⁷⁾، ونظيره «فايل فولت» (File Vault) من «آبل»⁽⁸⁾، القدرة على تشفير القرص الصلب بسهولة فائقة وشفافية كاملة. (في العام 2014، كنت أنصح برنامج «تروكربت» (TrueCrypt)، لكن المطورين توقفوا عن تطويره في تلك السنة تحت ظروف غامضة، ومن الصعب على الجميع إعطاء رأي حاسم بشأنه)⁽⁹⁾. تستطيع استخدام برامج تشفير «الدرشة» بواسطة الإنترنت كـ «أوف زي ريكورد» (Off the Record)، وهو سهل الاستعمال وآمن تماماً⁽¹⁰⁾. يستأهل برنامج «كريتوكات» (CryptoCat) بعض التفكير. إذا كنت تخزن معلوماتك على «سحابة» رقمية، اختر شركة تعطيك خيار التشفير. وشخصياً، أنا معجب ببرنامج «سبايدر رووك» (SpiderRoak)، لكن هناك برامج أخرى. هناك برامج لتشفير الصوت على الإنترنت كـ «سايلنت سيركل» (SilentCircle) و«تورفون» (TORFone) و«ريد فون» (RedPhone) و«بلاك فون» (Blackphone).

حاول إدخال مكوّن رقمي للاتصال بالإنترنت في البريد الإلكتروني، كـ «بي جي بي» (PGP). وحاضراً، يقدم «غوغل» بريداً إلكترونياً مشفراً لمستخدميه، وعلى الرغم من أنه يربك تنظيم الرسائل وعمليات أخرى، فإنه يزيد الخصوصية بما يجعله مجدياً⁽¹¹⁾.

يوصف «تي إس إل» (TSL) واسمه السابق «إس إس إل» (SSL) - بأنه بروتوكول يساعد على تشفير بعض عمليات التنقل على الإنترنت⁽¹²⁾. إنه ما يحدث أوتوماتيكياً في خلفية المشهد، عندما ترى رمز «إتش تي تي بي إس» (https) في بداية العنوان الإلكتروني للموقع الشبكي، بدلاً من «إتش تي تي بي» (http). يقدم العديد من المواقع الإلكترونية ذلك كخيار، ولكن ليس كصيغة افتراضية صحيحة. تأكد أنه يعمل بصورة مستمرة حين يمكنك ذلك، بوضع مكوّن رقمي للاتصال

في محرّك البحث بالإنترنت، يسمّى «إتش تي بي إس إفري وير» (HTTPS Everywhere)⁽¹³⁾.

ما سبق ليس لائحة حصرية؛ لأن وضعها يستلزم وضع كتاب سرعان ما تصبح معلوماته قديمة خلال شهور قليلة. إذ تتبدّل التكنولوجيا باستمرار، وعليك أن تذهب إلى الإنترنت للبحث عما يوصي به الخبراء⁽¹⁴⁾.

لن أتولّى قيادتك. هنالك عدد كبير من تقنيّات الـ «بت» تتخطى القدرات التقنية للقارئ العادي لهذا الكتاب. على وجه الخصوص، من المربك تماماً استعمال المكوّن الرقمي «بي جي بي»⁽¹⁵⁾. إن تقنيّات التشفير الأشدّ فعالية هي تلك التي تعمل في الخلفية حتى عندما لا تحس بوجودها، كـ «إتش تي بي إس إفري وير» وتقنيّات تشفير القرص الصلب. في الفصل 14، ناقشت أشياء تفعلها الشركات لتأمين بيانات مستخدميها. هناك أشياء أكثر من ذلك بكثير تجري في الكواليس. ثار سخط المؤسسات المعيارية الكبرى التي تدير الإنترنت بسبب رقابة الحكومة، إلى حدّ أنها تسعى إلى جعل التشفير موجوداً في الأمكنة كافة على الإنترنت⁽¹⁶⁾. ويؤمل أن تكون خيارات أخرى باتت متاحة عندما ينشر هذا الكتاب.

يستعصي معظم «البيانات الوصفية» على التشفير. لذا، تستطيع تشفير محتويات بريدك الإلكتروني، لكن يجب فك التشفير عند جهتي الإرسال والتلقي كي يعمل البريد الإلكتروني. وعلى نحو مُشابه، من المستطاع تشفير مكالماتك الصوتية، لكن إنجاز الاتصال يوجب عدم تشفير الرقم الذي تطلبه، وموقع هاتفك، وأرقام هوية هاتفك. وتستطيع تشفير معلومات بطاقتك الائتمانية عندما ترسلها بواسطة الإنترنت إلى أحد المحلات، تحتاج الشركة إلى اسمك وعنوان منزلك كي ترسل مشترياتك إليك.

وأخيراً، لا يحمي التشفير حاسوبك أثناء استعماله؛ فيبقى عرضة للاختراق من قبل المجرمين أو الحكومة. لكن، مرّة أخرى، يكون الشرط لحدوث ذلك أن تكون

مستهدفاً، لا أن تُصاب ضمن ضربة عامة. وتعني تلك الأشياء كلها أن التشفير جزء مهم من الحل، لكنه ليس الحل بأكمله.

حاضراً، يشكّل برنامج «تور» (TOR) أفضل أداة لحماية سرّية هويتك على الإنترنت. يتميّز بالسهولة في الاستعمال، وبقدر ما نعرف فإنه آمن. وكذلك من المستطاع استعمال هويّات بديلة للتهرب من الرقابة والحجب. يستطيع برنامج «أونيون شير» (Onionshare) إرسال الملفات بواسطة الإنترنت مع إغفال الهوية، بفضل برنامج «تور»⁽¹⁷⁾. وعلى رغم آراء مُعارضة، تمثّل الهويّات البديلة للخوادم وسيلة ناجعة لإغفال الهوية⁽¹⁸⁾.

ثمة أشياء بسيطة تستطيع استخدامها في صدّ الرقابة. تستطيع إيقاف خيار «خدمات الموقع» على هاتفك الذكي عندما لا تكون بحاجة إليها. حاول الحصول على معلومات كافية قبل اتّخاذ قرار أن تضع على هاتفك تطبيقاً رقمياً يطلب موقعك وبيانات أخرى. بإمكانك التوقّف عن وضع معلومات مُعرّفة في حساباتك على المواقع العامة. عندما التقى إدوارد سنودن الصحافيتين للمرّة الأولى في هونغ كونغ، أرغمهم على وضع هواتفهم النّقالة كلها في ثلاثة لحجب إشاراتنا الصادرة والواردة، فلا تكون الهواتف أدوات إصغاء تعمل عن بُعد⁽¹⁹⁾.

أحياناً، يكون صدّ الرقابة أمراً سهلاً تماماً. يكفي وضع لاصق فوق كاميرا الكمبيوتر فتكف عن التقاط الصور لمصلحة طرف استطاع أن يسيطر عليها عن بُعد. بإمكانك عدم وضع عنوان المُرسَل على مغلف الرسالة البريدية الورقية، فتقلّص من المعلومات التي يعرفها مكتب البريد عنك. تستطيع استئجار شخص ليسير خلف سيارتك فلا تلتقط كاميرات المراقبة لوحة أرقامها الخلفية، وهو ما يفعلُه البعض في طهران⁽²⁰⁾. أحياناً، يكون الأمر بمثل سهولة أن تقول «لا»، المقصود بذلك هو النأي بالنفس عن إعطاء معلومات شخصية على الاستمارات، وعدم إعطاء رقم هاتفك الخلوي لعامل المبيعات في المخزن وغيرها.

بعض أنواع صدّ الرقابة تكون غير مشروعة: ليس مسموحاً لك بأن تغطّي فعلياً لوحة أرقام سيارتك؛ كما أن بعضها مستهجن اجتماعياً كالتجول بين الناس مع ارتداء قناع؛ فيما أنواع أخرى ربما تجعلك عرضة للاستهزاء، كطلي الوجه بالصبغة كي لا تتعرّف الكاميرات إليه⁽²¹⁾، أو ارتداء ملابس معينة لتضليل طائرات الـ «درون»⁽²²⁾.

تشويه الرقابة. أنا أستخدم محرك بحث عملت على ضبط إعداداته كي تسمح الـ «كوكيز» في كل مرة أُغلّقه فيها، وهو ما يتكرّر مرّات عدّة يومياً. ولا يعني ذلك سوى أنني لا زلت خاضعاً للرقابة، لكن صار من الصعب تنسيق كل تلك الرقابات الصغيرة التي تجريها الـ «كوكيز» معاً لتعمل ضديّ، وكذلك لا تتبني الإعلانات. عندما أتسوّق من مخازن «سافواي»، أستخدم بطاقة صديقتي، وهي بطاقة من النوع التي يصدرها المخزن نفسه لمن يكرّر الشراء منه. ويؤدّي ذلك إلى تشويه معلومات الرقابة عنها.

أحياناً يسمّى ذلك «تعمية»، وتشمل خدعاً كثيرة تستطيع أنت ابتكارها، عندما تبدأ بالتفكير في الأمر⁽²³⁾. يمكنك أن تتبادل بطاقات «المقربون» التي تعطيها المخازن الكبرى إلى زبائنهم الدائمين مع أصدقائك وجيرانك. تستطيع أن ترتدي ملابس تجعل مظهرك ملتبساً. في رواية الأخ الصغير (Little Brother) للكاتب كوري دوكتورو، يعتمد بطل الرواية إلى وضع حجارة في حذائه كي يغيّر مشيّه ويجدع نُظم التعرّف إلى طريقة المشي⁽²⁴⁾.

هناك أمان في الأرقام أيضاً. كلما كان هنالك أمكنة في العالم تعمل فيها تقنيات الـ «بيت» على إنقاذ الناس، وزاد استخدامنا لها؛ صارت أكثر أمناً. يشبه ذلك مغلفات الرسائل الورق. لو تكاثر عدد مستخدمي البطاقات البريدية إلى حدّ أن تصبح القاعدة الأساسية في التراسل، يصبح مستخدمو المغلفات موضع شبهة. لكن، لأن معظم الناس يستعمل المغلفات الورق، لا يصار إلى الاشتباه في من

يستعملون مغلفات الورق للحصول على الأمان لرسائلهم. ينطبق ذلك خصوصاً على برامج إخفاء الهوية كـ «تور»، الذي يعتمد على عدد الناس الذين يستخدمونه كي يستطيع إخفاء هويتهم جميعاً.

تستطيع أيضاً، وأنا أعرف أشخاصاً يفعلون ذلك، البحث عن أسماء عشوائية على «فيسبوك» كي تضلل من يسعى إلى معرفة مَنْ تعرفهم فعلياً. في أفضل الحالات، يمثل ذلك حلاً جزئياً؛ لأن تحليل المعلومات يحتاج إلى التمييز بين الإشارات التي تحمل بيانات، والإشارات ذات الدلالة العشوائية التي تشبه الضوضاء؛ ما يعني إضافة مزيد من الضوضاء وتصعيب مهمة تحليل البيانات.

تستطيع أن تعطي معلومات مغلوطة عنك للاستمارات على الـ «ويب»، أو كلما طُلب منك. (تذكر أن أطفالك يفعلون ذلك طوال الوقت) ⁽²⁵⁾. لمدة سنوات، قبل زمن من رواج عمليات تتبع المستهلكين، كانت سلسلة مخازن «راديو شاك» (Radio Shack) تطلب روتينياً من الزبائن أرقام هواتفهم وعناوين بيوتهم. رفضت ذلك فترة، لكن ذلك بدا مستهجناً اجتماعياً ⁽²⁶⁾. وبدلاً من ذلك، اعتدت أن أعطي العنوان التالي: «9800، سافاج روود، كولومبيا، ولاية ميريلاند، 20755»، وهو عنوان مقر «وكالة الأمن القومي». وعندما أخبرت زميلاً لي بالأمر، أعلمني أنه يعطي العنوان الوهمي التالي: «1600، بنسلفانيا آفنيو، واشنطن، دي سي»، مصراً على أن أحداً لم يكشفه.

في وسعك الحصول على بطاقة ائتمان باسم ثانٍ. لا شيء سريٍّ في الأمر، إذ يكفي أن تطلب من شركة بطاقات الائتمان بطاقة أخرى باسم مغاير، مع بقائه مربوطاً بحسابك. وإذا لم يطلب البائع بطاقة الهوية منك، تستطيع استعمال تلك البطاقة.

يعطي الخداع نتائج مذهلة إذا مورس بتقشف وتقطّع. أتذكر قصة عن مجموعة نشطاء مغاربة. كانت الشرطة السرية تتعقب كل من لا يملك هاتفاً خلوياً منهم، ما يعرضه للضرب أيضاً. وعمد أعضاء المجموعة إلى اقتناء خلويات، لكنهم كانوا

يتركونها في المنازل عندما يريدون إخفاء تحركاتهم فعلياً. وبصورة أكثر تعمياً، إذا سدت على الرقابة المعادية الألفية كافة، تسد أمامك إمكانية خداعها أيضاً.

كسر الرقابة. استناداً إلى التكنولوجيا، تستطيع كسر أنواع من نظم الرقابة. بإمكانك قطع خطوط الكهرباء عن أجهزة مراقبة السرعة في الشوارع. تستطيع رش طلاء على عدسات كاميرات المراقبة. إذا كنت «هاكر» متمرس، تستطيع تعطيل نظم الرقابة على الإنترنت، حذف أو تشويش قواعد بيانات الرقابة، أو ممارسة أنواع أخرى من التخريب. لكن، توخ الحذر لأن معظم الأشياء التي وردت توأ هي غير قانونية.

بعض تلك السبل أكثر صعوبة من بعضها الآخر. سوف ينجز بعضنا أشياء أكثر من بعضنا الآخر. هناك من يعتمد على إدخال معلومات عشوائية في استمارات الإنترنت. حفنة ضئيلة من الناس - أنا لا أعرف سوى شخص واحد - تجري عمليات بحث عشوائية على «غوغل» للتشويش على بروفائلاتها في قواعد بيانات ذلك المحرك. يترتب على كثير من تلك الأشياء أكلافاً اجتماعية أو مالية أو هدرًا للوقت، إضافة إلى العبء النفسي للوقوع في برائن البارانونيا على مدار الساعة. شخصياً، نادراً ما أتقدم للحصول على بطاقات «المقربون» التي تعطيها المخازن الكبرى إلى زبائنهم الدائمين، ما يعني حرمانني من التخفيضات التي تمنح إلى تلك البطاقات. ولا أستخدم بريد الـ «جي ميل»، كما لا أدخل إلى بريدي الإلكتروني من الـ «ويب». لا أملك حساباً شخصياً على «فيسبوك»، ما يعني أنني غير متصل بأصدقائي بالطرق التي يتيحها ذلك الموقع. لكنني أحمل هاتفي الخلوي معي معظم الوقت، ويعني ذلك أن شركات عدّة تتبعني. ويستطيع كل امرئ اختيار ما يحلو له من السبل.

يجب على كل منا بذل قصارى جهده، استناداً إلى الإيمان بأن الخصوصية أمر مهم وأنه يجب أن نمارس حقوقنا تحت طائلة فقدانها⁽²⁷⁾. لكن، بحق السماء، لا

تعبثوا تلك الاستثمارات السخيفة على الإنترنت، إذا كنتم لا تعرفون إلى أين ستصل بياناتكم.

مساعدة رقابة الحكومة

ربما بدا أن إطلاق نداء لمساعدة جهود الحكومة في الرقابة أمر لا مكان له في الكتاب، لكن أصبحوا السمع إلى قليلاً.

هنالك حاجات مشروعة للرقابة الحكومية، تنبع من حاجات الاستخبارات وقوى إنفاذ القانون معاً، ويجب أن نقر بذلك. الأهم من ذلك أننا يجب أن ندعم الرقابة الشرعية، ونبحث عن طرق تمكن المؤسسات الحكومية من ممارستها دون أن تنتهك الخصوصية، وتخرب الأمن، وتتعدى على حق المواطن في التحرر من الرصد والاشتباه المفرط. إذا استطعنا إعطاء قوى إنفاذ القانون طرقاً جديدة للتحقيق في الجرائم، فسيكفون عن المطالبة بتهديم الأمن لمصلحتهم.

لن نخفي الصراعات الجغرافية-السياسية، وتشكل الاستخبارات الخارجية أداة متفرّدة في مواجهة تلك الحوادث⁽²⁸⁾. وفيما أكتب هذه الكلمات في صيف 2014، تحشد روسيا قواتها ضد أوكرانيا، وتنمر الصين على اليابان وكوريا في بحر الصين الجنوبي، ويقدم إرهابيو الـ «إيغور» على قتل صينيين من شعب الـ «هان»، وتهاجم إسرائيل غزة، وتساعد قطر وتركيا غزة للدفاع عن نفسها، وتتخبط أفغانستان في مათتها، وتفتت ليبيا، وتعود مصر إلى الديكتاتورية، وربما تعاود إيران برنامجها النووي، ويحتاج فيروس «إيبولا» غرب أفريقيا، وتختبر كوريا الشمالية صواريخ جديدة، وتقتل سوريا شعبها، ويهيمن على أجزاء كبيرة من العراق منظمة تنتمي اسمياً إلى التطرف الإسلامي وهي تعرف باسم «الدولة الإسلامية في العراق والشام». وليس ما سبق سوى ما يرد في نشرات الأخبار. وعندما تقرأ هذا الكتاب، ستكون القائمة مختلفة، لكنها لن تكون أقل فداحة. وأؤكد لك أن أحداً في البيت

الأبيض لن يدعو «وكالة الأمن القومي» إلى تقليص عملياتها في جمع المعلومات عن تلك التهديدات وما يشبهها. ويجب عليهم ألا يفعلوا.

إضافة إلى ذلك، يملك حكومات العالم دعر واسع من إمكان شن هجمات في الفضاء السبراني. يأتي معظم ذلك الدعر من رد فعل مبالغ فيه، لكن المخاطر حقيقية. ويتخبط الدفاع السبراني في مشكلة العمل الجماعي التقليدية. إذ تدير أيدي القطاع الخاص معظم البنية التحتية للفضاء السبراني، لكن معظم الضرر الذي ربما ينجم من هجمات سبرانية كبرى، سيحقيق بالجمهور ككل. ويعني ذلك أنه على المدى الطويل سيصعب الركون إلى الشركات التي تدير بنيتنا التحتية، لتقديم حماية مناسبة لتلك البنية. ثمة ضرورة لنوع من التدخل الحكومي. في 2013، صرح مدير «وكالة الأمن القومي» الجنرال كيث ألكسندر بالقول: «لا أستطيع الدفاع عن البلاد ما لم أدخل الشبكات كلها»⁽²⁹⁾. وتعتبر تلك الكلمات عن الرأي السائد في واشنطن.

نعم، يجب علينا الحسم بشأن المدى الذي نرغب فيه بوجود الوكالة في شبكاتنا كلها. لكن، يجب أيضاً أن نساعد الوكالة في ألا تطلب الدخول إلى شبكاتنا كلها. إذا استطعنا أن نقدم للحكومات طرقاً جديدة في الحصول على معلومات عن الدول العدوانية، والمجموعات الإرهابية وعناصر الإجرام العالمي؛ فلسوف تقل حاجتها إلى الإجراءات المشتطة التي وصفتها في هذا الكتاب. إنها دعوة أصيلة إلى أفكار وأدوات وتقنيات جديدة. بكل صدق، لا أعرف كيف ستكون الحلول. ثمة طريق وسط، ومنوط بنا جميعاً أن نعثر عليه. إذا أردنا من مؤسسات كـ «وكالة الأمن القومي» أن تحمي خصوصيتنا، يجب علينا أن نعطيها طرقاً جديدة لأداء عملها الاستخباراتي.

اختر حلفاءك وأعداءك

تستند قوانيننا إلى الموقع الجغرافي. ولفترات طويلة من التاريخ البشري، بدا ذلك الأمر منطقياً تماماً. ويبدو ذلك أقل منطقية عندما يتعلق الأمر بالإنترنت؛ لأن تلك الشبكة دولية جداً.

من الواضح أنك تخضع للقوانين الشرعية للبلد الذي تعيش فيه، لكن عندما تكون على الشبكة، تضحي الأشياء أكثر تعقيداً. إذ إنك تتأثر بقوانين البلد الذي يعيش فيه صنّاع المكوّنات الإلكترونية، وقوانين البلد الذي يستقر فيه الشركات التي تباع البرامج، والبلد الذي يقدم لك خدمة «حوسبة السحاب» بشبكة الإنترنت. وسوف تتأثر أيضاً بقوانين البلد الذي تستقر فيه الخوادم التي تحتزن معلوماتك وبياناتك، وقوانين البلدان التي تمرّ فيها بياناتك عندما تتحرك بخطوط الإنترنت⁽³⁰⁾.

مثلاً، يجبر «قانون باتريوت» الشركات الأميركية على تسليم بيانات إلى الحكومة الأميركية عندما تطلبها، بغض النظر عن مكان تخزينها. ربما تكون مواطناً فرنسياً تعيش في فرنسا، وتخزن «مايكروسوفت» بريدك الإلكتروني في خوادمها في أيرلندا حصرياً. ولكن، لأن «مايكروسوفت» شركة أميركية، تزعم الولايات المتحدة أن تلك الشركة مجبرة على تقديم بياناتك لها عند الضرورة⁽³¹⁾. وترغب المملكة المتحدة في امتلاك نفاذ مماثل⁽³²⁾.

ويعني ذلك أنه يجب عليك أن تختار أي البلدان تثق بها، وما هي الشركات التي تثق بها.

لا تتساوى الشركات كلها في السوء. تستطيع الحصول على البريد الإلكتروني والمفكرة ودليل العنوانين، إما من «غوغل» أو «آبل». سوف تحمي الشركات بياناتك من الجمع الجماعي في بلدان كثيرة، لكنهما ستسلمانها لحكومات عدّة إذا أجبرتاً قانونياً على ذلك. ينخرط «غوغل» راهناً في مشروع ضخّم لحماية بيانات مستخدميه من رقابة الحكومة. في المقابل، يجمع «غوغل» بيانات الجمهور ويستخدمها لغايات الإعلان، فيما تستند «آبل» إلى نموذج عمل مغاير يحمي خصوصية مستخدميها⁽³³⁾.

هل تثق بشركة في الولايات المتحدة لا قيود عليها في ما تستطيع عمله ببياناتك، إضافة إلى خضوعها لطلبات قانونية من الـ «إف بي آي» و«وكالة الأمن القومي»،

بخصوص تلك البيانات؟⁽³⁴⁾ أم تثق بشركة أوروبية تعمل ضمن قيود حكومية صارمة بشأن رقابة الشركات، لكنها تخضع لرقابة بلا قيود تمارسها حكومة بلدها والولايات المتحدة معاً، ما يعني أن بياناتك تعبر الحدود الدولية؟ إذا لم تشتري من شركة «سيسكو سيستمز» معدات تشبيك بسبب تخوفك من «الأبواب الخلفية» لـ «وكالة الأمن القومي»، فمن أين ستشتري معداتك؟ هل تلجأ إلى «هواوي» الصينية؟ تذكر التشبيه الذي أوردته في الفصل 4 عن الإقطاعية في العلاقة بين الجمهور والشركات؛ أي السادة الإقطاعيين تثق به أكثر؟

يصعب تحديد نقطة البداية. ففي عالم «حوسبة السحاب» حاضراً، لا نعرف أي الشركات تستضيف معلوماتنا فعلياً. إن شركة إنترنت كـ «أوربيتز» (Orbitz) تملك بنية تحتية تستضيفها خوادم شركة «أتلاسيان» (Atlassian) التي تحصل على بنيتها التحتية من مقدم خدمات إنترنت كـ «راك سبائس» (Rack-Space)؟ فهل لك أن تعرف أين تكون فعلياً بياناتك المخزنة لدى «أوربيتز»؟

يجب أن نمتلك القدرة على معرفة أين نخزن بياناتنا ومعلوماتنا فعلياً، وتعيين البلد الذي نرغب في تخزين معلوماتنا فيه، والبلد الذي لا نرغب في أن تكون بياناتنا قريبة منه. في الوقت عينه، يجب أن نبذل قصارى جهدنا. وفي معظم الأحيان، يجب أن نعترف ببساطة أننا لا نعرف.

لكن، عندما يتعلق الأمر بالحكومات، أنا مضطر للقول بأسف إنني أفضل أن تتجسس علي حكومة الولايات المتحدة، أكثر من أي نظام آخر.

حرض على التغيير السياسي

في العام 2014، ألغت «محكمة العدل الأوروبية» قوانين الاتحاد الأوروبي المتعلقة بتخزين البيانات، وكانت تفرض على مقدمي خدمات الإنترنت الاحتفاظ بالبريد الإلكتروني والبيانات عن المكالمات الهاتفية، لمدة سنتين⁽³⁵⁾. في ردة فعل،

سارعت الحكومة البريطانية إلى إقرار قانون جديد أعاد فرض تلك المدّة على تخزين المعلومات، كما أعطيت الشرطة صلاحيات جديدة في رقابة المواطنين⁽³⁶⁾. بدا ذلك قيداً سياسياً كريهاً، لكن المثير هو الطريقة التي برّر بها رئيس الوزراء البريطاني ديفيد كامرون ذلك القانون في أحد برامج الراديو⁽³⁷⁾. إذ قال: «ببساطة، لست مستعداً لأن أكون رئيس الوزراء الذي يتحدث إلى الناس بعد ضربة إرهاب مبيّناً لهم أنه كان بوسعنا فعل المزيد في الحيلولة دونها».

لا يعدو ذلك كونه خطاب الخوف، لكنه ليس خوفاً من الإرهابيين. إنه الخوف السياسي من تحمّل الملامة إذا حدثت ضربة إرهاب. يرغب السياسيون في فعل أي شيء بغض النظر عن كلفته وقدرته فعلياً على جعل الناس أكثر أمناً، وأثاره الجانبية؛ كي يتجنّبوا الملامة عن كونهم لم يبذلوا جهداً أكبر. يفسّر ذلك الخوف معظم السياسة التي انتهجت بعد 9/11، وغالبية برامج الرقابة العامة التي مارستها «وكالة الأمن القومي». يملك سياسيون الرعب من ملامتنا لهم بأنهم لم يفعلوا كل ما قالت وكالات الاستخبارات أنه واجب على السياسيين فعله لتجنّب مزيد من الإرهاب. يجب علينا إقناعه وبقية مواطنينا الناخبين، بأنه يتعين عليه فعل الأمر الصحيح مهما كان شأنه.

معظم الحلول التي عُرضت في الفصلين السابقين تتطلّب من الحكومات إما تفعيل القوانين السارية أو تغيير القانون. وإلى حدّ كبير، لن يحدث أيّ من الأمرين ما لم نطالب بذلك. يتردّد السياسيون في خوض تلك النقاشات، ويتدّدون أكثر في تفعيل قيود مجدية على رقابة الحكومة. وبطبعهم، يبدي المشرّعون احتراماً خاصاً لطلبات قوى إنفاذ القانون، ويوظّف المجتمع الصناعي - الرقابي مجموعات ضغط لمؤازرتهم. لا يرغب أحد في الظهور بمظهر الضعيف حيال الجريمة والإرهاب. وحاضراً، عندما ضبطت وكالات الاستخبارات الأميركية أثناء تجاوزها القانون، لا يتهدّد السجن أحداً سوى من أطلقوا صافرات الإنذار حيال ذلك.

من جهة الشركات، تبذل مجموعات الضغط السياسي قصارى جهدها لضمان عدم حدوث إصلاح جذبي بشأن الرقابة التي تمارسها الشركات. ترفع حرية السوق مبرراً لاستمرار ذلك الشلل. وكذلك تضغط قوى الأمن وأجهزة الأمن القومي كي تضمن بقاء بياناتنا في متناول أيديها.

إذا أردنا أن يصوّت مشرّعونا ضد المصالح القويّة للعسكر وقوى إنفاذ القانون والشركات المثقلة بمجموعات الضغط (سواء التي تمّد الحكومة بالبيانات أم تلك التي تتجسّس علينا مباشرة)؛ يجب أن نجعل من أنفسنا أقوياء. ويعني ذلك أنه يجب علينا الانخراط في العملية السياسيّة. ولديّ في ذلك 3 توصيات محدّدة.

لاحظ وجود الرقابة. إنّها الخطوة الأولى. لا يتبدى معظم الرقابة للأعين، لكنه ليس خفياً كليّاً. ربما كانت الكاميرات صغيرة، لكنك تستطيع ملاحظتها إذا حدّقت. تستطيع أن تلاحظ مَنْ يقوم بالمسح الضوئي لبطاقة هويتك عندما تدخل المقصف. تستطيع وضع مكوّن داخلي في متصفحك كي تعرف من يلاحقك على الإنترنت. بإمكانك التنبّه للأخبار عن الرقابة. هناك مواقع على الإنترنت تعرف بكاميرات المراقبة⁽³⁸⁾. كلما عرفت أكثر، يتحسّن فهمك لمجريات الأمور.

تحدّث عن الرقابة. إنّها الخطوة الثانية. كلما زاد حديثنا عن الرقابة، ازداد الناس إدراكاً بمجرياتهما. وكلما ازداد ذلك الإدراك، يصبح الناس أكثر اهتماماً بها. وكلما تحدّثنا عن الرقابة علانية، يدرك مشرّعونا أكثر أننا نهتم لأمرها.

أقصد ذلك بصورة عامة تماماً. تحدّث عن الرقابة إلى عائلتك وأصدقائك وزملائك. لا تكن من أولئك المزعجين الذين لا يضعون تدوينات إلا عنها، لكن تشارك بها يرد في الأخبار عنها بوسائل الـ «سوشال ميديا». انضم إلى التجمّعات، ووقّع على البيانات العامة بصددّها. اكتب إلى ممثلك في البرلمان. أعطِ نسخاً من هذا الكتاب إلى أصدقاء كهدايا. لتكن آراؤك معروفة. إنّها أشياء مهمّة.

تحدّث عن القوانين في بلادك. ما هي أنواع الرقابة المشروعة في موطنك؟ كيف تتدخّل مصالح رجال الأعمال فيها، وما هو نوع الرقابة المتاحة لهم قانونياً؟ ما هي الحقوق التي يملكها الناس في استخدام أدوات تمكين الخصوصية؟ ابحث عنها.

تتمثّل إحدى المناحي الأكثر سوريالية التي أظهرتها كشوفات سنودن عن «وكالة الأمن القومي»، في أنها جعلت نظريات المؤامرة الأكثر انغماساً في البارانويا تبدو كأنها نص متماسك من العقلانية والحسّ السديد. من السهل نسيان تلك التفاصيل، والعودة إلى الإحساس بالرضى؛ لذا فإنّ استمرار النقاش عن تلك التفاصيل هو وحده الكفيل بالحيلولة دون ذلك.

تنظّم سياسياً. إنّها استراتيجيتنا الأشدّ فعالية. ثمة أمثلة حديثة عن كيفية انتظام الناس سياسياً ضد الرقابة. ففي كوريا الجنوبية، احتجّ الأساتذة على وضع قواعد بيانات جديدة عن الطلبة⁽³⁹⁾. واحتجّ المستهلكون الألمان على وضع عربات مزوّدة بنظام «رفيد» تسمح البضائع والأقسام والرفوف التي يمرّون بها أثناء تجوالهم في المخازن الكبرى⁽⁴⁰⁾. كما احتجّ مستخدمو «فيسبوك» على فرض شروط استخدام جديدة في صفحاتهم⁽⁴¹⁾. واحتجّ مسافرون مع شركات الطيران الأميركية على استعمال ماسحات ضوئية تصور الجسد بأكمله⁽⁴²⁾. لا تتكلّل حملات الاحتجاج بالنجاح دوماً، كما أن نتائجها بعيدة عن الكمال، لكن من النافل الإشارة إلى الأهمية التي يكتسبها التحرك جماعياً. يجب أن نعي بأن تلك الأمور تطالنا جميعاً، وحلولها تكون عامة أيضاً.

ليس هذا بكتاب عن كيفية التنظيم سياسياً، وهناك أشخاص أكثر تمرّساً مني بكثير في شرح كيفية تحريك التغيير السياسي. أعرف أن السياسات هي أمور لا تحصل أثناء الانتخابات وحدها. بالأحرى، إنّها عملية مستمرة، وتشمل الانخراط مع المشرّعين، والاحتجاج علناً، وتقديم الدعم لمجموعات لا تسعى إلى الربح وتنشط في ذلك المجال. انظر إلى «مؤسسة الحدود الإلكترونية» (Electronic Frontier Foundation)

و«مركز معلومات الخصوصية الإلكترونية» (Electronic Privacy Information Center) و«مركز الديمقراطية والتكنولوجيا» (Center for Democracy & Technology) و«المنظمة الدولية للخصوصية» (Privacy International) و«معهد التكنولوجيا المفتوحة» (Open Technology Institute) وغيرها. تكافح تلك المجموعات كلها من أجل رقابة أقل وخصوصية أكثر. ادعمها.

لا نستطيع فعل الكثير في بقية أرجاء العالم [أي خارج الولايات المتحدة]، لكننا نستطيع أن ندفع باتجاه التغيير حيثما نقدر على ذلك. بعدها، نستطيع التحرك ببطء نحو الخارج. هكذا يحدث التغيير عالمياً⁽⁴³⁾.

لا تستسلم. القدرة عدوة التغيير. تتبدى القدرة في القول بأن الحكومات والشركات الكبرى تملك أسباب القوة كلها، ومعظم السياسيين ليست لديهم الرغبة في تقيدهما؛ ما يعني أننا عاجزون عن تغيير الأشياء. وكذلك تتبدى القدرة في القول إن الرقابة الشاملة هي كلية القدرة إلى حدّ أننا لا نستطيع مقاومتها، بل إن من شأن المقاومة أن تضعنا قيد اهتمامها على كل حال.

تحمل تلك التأكيدات شيئاً من الحقيقة، لكن خلاصاتها مغلوبة. فمن شأن الأمن الجيد للكمبيوتر والانتشار الواسع للتشفير، تصعيب مهمة الرقابة العامة. ومن شأن العمل على التعاون انتقائياً مع الشركات على أساس سياساتها في الخصوصية؛ جعل الشركات أكثر ميلاً للسياسات الحسنة بصدد الخصوصية. وبمرور الوقت، سيخفت افتتاننا بـ«البيانات الضخمة» وخوفنا غير المعقلن من الإرهاب. وفي نهاية الأمر، سوف تعمل القوانين على تقييد سلطة الحكومة والشركات معاً على الإنترنت.

يمثل ما أوصي به نقلات كبرى سياسياً، تستلزم بذل كثير من الجهد. وتاريخياً، عُدَّت النقلات السياسية الكبرى عبثية في بداياتها. تلك هي طريقته. يجب أن نقاتل

من أجل التغيير السياسي، ونستمر في القتال حتى نتصر. وحتى ذلك الحين، هنالك كثير من المعارك الصغيرة التي يجب أن نكسبها.

هناك قوة في الكثرة، فإذا تصاعد صوت الجمهور، سوف تُجبر الشركات والحكومات على الاستجابة له. ما نحاوله هو منع ظهور حكومة شمولية من النوع الذي رسمته رواية جورج أورويل 1984، وكذلك الحيلولة دون سلطة تديرها الشركات، على غرار ما رسمته مجموعة كبيرة من روايات الخيال العلمي المتشائمة المنتمية إلى ثقافة الـ «بانك السبراني»^(*) (Cyberpunk).

وبأي حال من الأحوال، لسنا قريبين من النهايتين، لكن القطار يتحرك في اتجاههما معاً، ويجب علينا تشغيل المكابح.

(*) ظهرت حركة الـ «بانك» الشبابية المتمردة في ثمانينيات القرن العشرين، خصوصاً في بريطانيا أيام رئيسة الوزراء الراحلة مارغريت تاتشر. كانوا متشائمين بمسار المجتمعات الغربية وثقافتها. واشتهروا بقصّات الشعر التي تشبه عُرف الديك، والأوشام الكثيرة على الجسد، ووضع الغرسات المعدنية في الأنوف، والموسيقى التي تمزج الصخب بالكآبة. لاحقاً، صار كثير من الـ «بانك» رواداً مؤسسين في المعلوماتية في أميركا، وحملوا شيئاً كثيراً من ثقافة التمرد إليها.

16

الأعراف الاجتماعية ومقايضة «البيانات الضخمة»

في الفصول الثلاثة السابقة، تحدّثت عن الحاجة إلى إجراء تغييرات كثيرة: في الحكومة والشركات والسلوك الفردي. كان بعض التغييرات تقنياً، لكن معظمها يتطلب قوانين جديدة أو على الأقل سياسات جديدة. في هذا الوقت، يبدو معظمها غير واقعي، على الأقل في الولايات المتحدة. إذ أعيش في بلد ما زالت غالبية السكان فيه لا تطالب بتلك التغييرات، إضافة إلى أنّ ذلك البلد لا تترجم فيه إرادة الناس بسهولة إلى أفعال تشريعية.

تبدو غالبية الناس [في الولايات المتحدة] غير مبالية بأن تجمع الشركات تفاصيلها الحميمة وتستخدمها أيضاً، معتقدة بأن الرقابة التي تمارسها حكومات يتقنون بها تمثّل شرطاً أساسياً لحفظ أمنهم. ما زال معظم الناس يخاف الإرهاب بشكل مبالغ فيه. ولا يفهم الناس المدى الذي بلغته قدرات الرقابة عند الحكومة والجهات الخاصة. يقلّلون من شأن الرقابة الجارية، غير مدركين أن الرقابة الحكومية العامة لا تحفظ أمن غالبيتنا. ويبدو معظم الناس مرتاحاً إلى مقايضة بياناته الحساسة بالحصول على بريد إلكتروني ومحرك بحث على الإنترنت أو منصّة للثرثرة مع أصدقائه.

يختلف الوضع في أوروبا إلى حدٍّ ما؛ لأنها تفرض قوانين أشد صرامة على الشركات وتمارس حكوماتها رقابة أقل، لكن مشاعر عامة الناس تتشابه مع ما في الولايات المتحدة إلى حدٍّ كبير.

قبل أن نتوصل إلى تغيير سياسي، يفترض ببعض من قيمنا الاجتماعية أن تتغير. يجب أن نصل إلى نقطة يدرك الناس فيها المدى الفائق الاتساع للرقابة، وما يولده ذلك من تمركز فائق للقوة والسلطة. عندما يفعلون ذلك، ربما قال معظم الناس: «ذلك الأمر ليس سليماً». يجب أن نستجمع القوة السياسية لنقارع قوى إنفاذ القانون ووكالات الاستخبارات القومية من جانب الحكومة، وكذلك المتعاقدين مع الحكومة وصناعة الرقابة من جهة الشركات. وقبل حدوث أيٍّ من الأمرين، يجب إحداث تغييرات كبرى في طريقة نظر المجتمع للخصوصية وكيفية تقييمه للخصوصية والأمن والحرية والثقة، إضافة إلى حفنة من المفاهيم المجردة التي تحدّد ذلك النقاش.

إنّه لأمر صعب. إذ تميل المشاعر السياسية إلى التحرك باتجاه الممارسة العملية. نحن ماهرون في قبول الأمر القائم، أيّاً كان ومهما كانت جذته. (للأمانة، يطيح بعقلي أن كل تلك الرقابة ظهرت في أقل من عقدين). بتنا ننمو في ظل تعودنا على الـ «بان أوبتكون»^(*). بوسعك أن تراه يتضخّم باستمرار فيما الناس يهزّون أكتافهم قائلين: «ما الذي تنوي فعله؟» بوسعك أن تراه على المستوى الصغير في كل مرة يعتمد فيها «فيسبوك» إلى الانحدار بمستوى الخصوصية عند استخدامه: في البداية يتدمّر الناس، وسرعان ما يعتادونه.

تتناول بقية هذا الفصل كل التغيرات اللازمة في السلوك. هناك طُرُق يجب اتباعها لتعديل مشاعرنا وأفكارنا، إذا قيّض لنا الخروج من آسار مجتمع الرقابة.

إعادة صوغ معايير خوفنا

وُقّع «قانون باتريوت» في 26 تشرين أول (أكتوبر) 2001، بعد 45 يوماً من هجمات الإرهاب ضد البنتاغون ومركزي التجارة العالميين. لم يكن سوى «قائمة أمنيات» الشرطة والسلطات وقوى الاستخبارات، ومُرّر بأغلبية ساحقة في مجلسي النواب والشيوخ، وبحد أدنى من النقاش. لم يقرأه أحد في الكونغرس قبل التصويت عليه⁽¹⁾. وتقريباً، كان كل الناس راغبين في إقراره، على الرغم من عدم فهم إملاءاته⁽²⁾.

في 2014، حضرت نقاشاً تحدّث فيه تيم دافي، الرئيس والمدير التنفيذي لوكالة الإعلانات «إم إند سي ساتشي» (M & C Saatchi)، وحاول فيه تقديم رسالة محسّنة عن الخصوصية⁽³⁾. وسأل: «أين ترسم خط الفصل؟» في محاولة لرسم صيغة عن الخصوصية. لكن، إذا كان المستمعون في ذعر من الإرهابيين، فلسوف يرسمون الخطوط بما يسمح بالكثير جداً من الرقابة⁽⁴⁾. وأشار جاك غولد سميث أستاذ القانون في «جامعة هارفرد»، إلى أنّه عندما نكون مذعورين، تؤدّي زيادة إشراف الكونغرس إلى إعطاء مزيد من الصلاحيّة إلى «وكالة الأمن القومي»⁽⁵⁾.

يتقدّم الخوف على الخصوصية⁽⁶⁾. يتقدّم الخوف من الإرهاب على الخوف من الطغيان. إذا بلغ من القوة مبلغاً كافياً، فلسوف يتقدّم على الحجج التي جمعها الكتاب كافة⁽⁷⁾. بالنسبة للناس، إنّه الخوف من ضربة الإرهاب المقبلة. بالنسبة للسياسيين يكون الأمر كذلك، إضافة إلى الخوف من تلقي الملامة عن ضربة الإرهاب التالية. لكنه الخوف، في كل الأحوال. لتذكّر حديث رئيس الوزراء كامرون الذي ورد في الفصل السابق. إنّه ما أسمعه مراراً وتكراراً من مسؤولين حكوميين عندما أسألهم عن وضوح انعدام فعالية الرقابة العامة في مواجهة خطر الإرهاب. وإذا يقرّون بذلك، إلاّ إنهم يرون في الرقابة العامة سياسة ضمان. ويعرفون أن جهودهم في الرقابة الموجهة سوف تفشل عند نقطة ما، ويعقدون الأمل على أن تكون الرقابة

العامة حاضرة كاحتياط. يصح القول حقاً إن الاحتمالات ضئيلة بأن تكون فعّالة على ذلك النحو، لكنهم [المسؤولين الحكوميين] يعتقدون بأنه يجب عليهم فعل كل شيء ممكن، من أجل أمن البلد وأمن مناصبهم معاً⁽⁸⁾.

وبغض النظر عن مدى الخطر، لا تمثل الرقابة العامة إجراءً مضاداً فعّالاً؛ فيما تتسم بالفعالية عمليات الاستخبارات وإجراءات الشرطة. يجدر بنا مقاومة النزعة إلى القيام بشيء ما، بغض النظر عما إذا كان العمل المقترح فعّالاً أم لا.

يمثل الإبقاء على الخوف متأججاً تجارة هائلة⁽⁹⁾. يعرف العاملون في مجتمع الاستخبارات أنه أساس نفوذهم وقوتهم. ويعلم المتعاقدون مع الحكومة أنه مصدر الأموال لعقودهم. ولاحظ الكاتب والناشط على الإنترنت كلاي شيركي أنّ «المؤسسات ستحاول الحفاظ على المشكلة التي تمثل [تلك المؤسسات] حلاً لها»⁽¹⁰⁾. الخوف هو تلك المشكلة.

إنه الخوف الذي تؤججه نشرات الأخبار يومياً. وبمجرد حدوث جريمة مرعبة أو هجوم إرهابي يفترض أنه كان ممكناً منعه بمجرد إعطاء الـ «إف بي آي» أو «وزارة الأمن الوطني» نفاذاً أكبر إلى بعض المعلومات المخزنة في «فيسبوك» أو المشفرة في «آي فون»؛ يضحي مطلب الناس هو أن يعرفوا لماذا لم تحصل الـ «إف بي آي» أو «وزارة الأمن الوطني» على حق النفاذ إلى تلك المعلومات، ولماذا جرى منعهم من «الوصل بين النقاط». وعندها، تتغير القوانين كي تعطيهم مزيداً من السلطة. وبالعودة إلى جاك غولد سميث، فإنه يقول: «ستزيد الحكومة من سلطاتها كي تستطيع ملافاة التهديد للأمن الوطني (لأن الناس يريدون ذلك)»⁽¹¹⁾.

نحتاج إلى طريقة أفضل في التعامل مع ردود أفعالنا العاطفية حيال الإرهاب، تكون غير إعطاء حكومتنا شيكاً على بياض في التعدي على حرياتنا، في محاولة يائسة لاستعادة الشعور بالأمن. إذا لم نعثر على أي طريقة لفعل ذلك، فعندها يمكن أن يقال إن الإرهاب حقق نجاحاً حقيقياً. أحد أهداف الحكومة هو إعطاء الأمن

لشعبها، لكن في الديمقراطيات، يجب علينا خوض المخاطر⁽¹²⁾. عندما يرفض المجتمع المخاطرة - في الجريمة والإرهاب وغيرهما - يكون دولة بوليسية بالتعريف. وتحمل الدولة البوليسية مخاطرها الخاصة أيضاً.

لا ينحى باللائمة على السياسيين وحدهم في ذلك⁽¹³⁾. الإعلام العام مُدانٌ أيضاً. وبتركيزه على الحوادث النادرة والمشهدية، يولد الإعلام لدينا رد فعل شرطي للتصرف كأنها الإرهاب شيء شائع أكثر مما هو عليه فعلياً، ولخشيتيه بأكثر من نسبة حدوثه فعلياً. وكذلك نُلام نحن أيضاً، إذا اشترينا البروباغندا التي يبيعنا إياها الإعلام.

علينا أيضاً أن نعارض مفهوماً مفاده أنّ التكنولوجيا الحديثة تجعل الأشياء كلها مختلفة⁽¹⁴⁾. في الأيام والأسابيع التي تلت هجمات الإرهاب في 9/11، عندما خضنا في نقاش عن قوانين جديدة وسلطات جديدة للأمن؛ سمعنا العبارة التالية: «الدستور ليس حلفاً انتحاريّاً». إنّها تعبر عن مشاعر منغمسة في الخوف، ويجدر تبيان معناها⁽¹⁵⁾. يشبه ما تقوله تلك العبارة ما يلي: «الناس الذين كتبوا قوانيننا لم يكن لهم أن يتوقعوا الوضع الذي نواجهه الآن. لذا، فإن القيود التي فرضوها على سلطات الشرطة وقوى الأمن، والنواهي التي فعلوها ضد الرقابة، لا تنطبق علينا. إنّ وضعنا متفرد، وعلينا تجاهل تلك الأمور كلّها». تمثل السبب الرئيس في استسلامنا لتلك المفاهيم في اعتقادنا بأن الضرر الذي يستطيع الإرهابيون التسبب به، هو من الضخامة بما يجعل من غير المفهوم أن نركن إلى الوسائل التقليدية في إنفاذ القانون، والمحاكمات المبنية على الوقائع.

إنّ ذلك ليس صحيحاً أبداً. إنّها مغالطة نفسية شائعة الاعتقاد بأننا نعيش أوقاتاً فائقة الفرادة، وأنّ تحدياتنا لا تشبه ما قبلها إطلاقاً، ما يوجب تجاهل الضوابط الاجتماعية التي وضعناها قبلاً للحدّ من قوة السلطات الحكومية. استسلم الرئيس إبراهيم لينكولن لتلك المغالطة عندما أوقف العمل بإصدار مذكرة قانونية كشرط

لمثول شخص ما أمام المحكمة، أثناء الحرب الأهلية. وتكرّر الأمر عينه مع الرئيس وودرو ويلسون عندما اعتقل ورّحل قادة العمّال والاشتراكيين بعيد الحرب العالمية الأولى مباشرة. وفعل الرئيس فرانكلين روزفلت الأمر عينه عندما احتجز أميركيين من أصول يابانية وألمانية وإيطالية، أثناء الحرب العالمية الثانية. وكرّرنا ذلك في الحقبة المكارثية أثناء الحرب الباردة. وها نحن نفعلها كرّة أخرى بعد 9 / 11.

لا يشكل الخوف طريقاً وحيداً للرد على تلك التهديدات، وهناك حالات كثيرة لم تتخل فيها المجتمعات عن حقوقها، في سياق سعيها إلى البقاء آمنة. ففي خضم المجزرة المروّعة في النرويج التي ارتكبها أندرياس بريفيك، حافظت تلك البلاد إلى حد كبير على قيمها الأساسية في الحرية والانفتاح⁽¹⁶⁾. وهناك الجملة الشهيرة للرئيس فرانكلين دوايت روزفلت نفسه: «الشيء الوحيد الذي يجب أن نخاف منه، هو الخوف نفسه». أن لا نهزم، هو رد الفعل الصحيح على الإرهاب⁽¹⁷⁾.

ثمة أمل للولايات المتحدة⁽¹⁸⁾. لم يكن الخوف رد فعلنا دائماً على الإرهاب. وباسترجاع التاريخ الحديث، فإن الرؤساء الذين قاوموا الإرهاب - ترومان، آيزنهاور، نيكسون، وريغان أحياناً، وبوش الأب - حقّقوا نتائج عملية وسياسية أفضل من أولئك الذين اتخذوا الإرهاب ذريعة للحصول على مظلة سياسية: كارتر، ريغان (معظم الوقت)، وبوش الابن. نحتاج إلى الإقرار بقوة السياسيين الذين يحمون حريّاتنا أثناء المخاطر، وضعف السياسيين الذين يعجزون عن حلّ المشاكل فيختارون التضحية بحريّاتنا. بعد ما يزيد على عقد من 9 / 11، أزعج الوقت للتحرك بعيداً من الخوف، ونعود إلى القيم الأميركية الأساسية في الحرية والتحرّر والعدالة⁽¹⁹⁾. وثمة مؤشرات على أننا نفعل ذلك. ففي 2013، شرعنا في رؤية انزياح لافت في مدرّكات الأميركيين عن قبول مبادلة الحريّات المدنية بالأمن القومي⁽²⁰⁾.

إعادة صوغ معايير الخصوصية

تتسم تعريفاتنا الشخصية للخصوصية بأنها ثقافية ووظيفية في آن معاً. إذ كانت مختلفة قبل 100 سنة عن حالها حالياً، ولسوف تكون مختلفة أيضاً بعد 100 سنة من الآن. وتختلف في الولايات المتحدة عما هي عليه في أوروبا واليابان وأمكنة أخرى⁽²¹⁾. كما أنها تتفاوت بين الأجيال.

وحاضراً، تؤثر الإنترنت في توجهاتنا حيال الخصوصية، بطريقة غير مسبقة. ويرجع ذلك إلى أن الطرق الرئيسة التي نستخدمها تتمثل في التعلم من بعضنا بعضاً. إذ يتصيد المحامون المحلفين المحتملين، ويتتبع الباحثون عن وظيفة المدراء التنفيذيين، وترصد أقسام الموارد البشرية في الشركة بالمتقدمين إلى الوظائف⁽²²⁾. قبل المواعيد الأولى، يترصد الناس ببعضهم بعضاً⁽²³⁾. حتى إن ذلك الشيء له اسم: قسم التريص في محرك البحث «غوغل»⁽²⁴⁾.

على خطوط الإنترنت، نسبر غور الأشياء باستمرار، وأحياناً يتعدى أحدنا على خصوصية الآخر. يمكن ألا يكون ذلك مريحاً أبداً. تعطي الطبيعة شبه الأبدية للاتصالات على الإنترنت فرصاً من الأنواع كافة لمن يريد أن يضايقك. وبسهولة، يمكن تحويل رسائل الـ «إيميل» التي أرسلتها إلى أحدهم بصورة شخصية، كي تصبح في متناول آخرين. وباستمرار، يفعل الأطفال حاضراً ذلك الأمر ببعضهم بعضاً. إذ يحولون لبعضهم بعضاً المحادثات الخاصة والصور والرسائل، أو يظهرون التدوينات التي كتبت بصورة شخصية على مواقع الـ «سوشال ميديا». ومن أسباب إقبال الشباب والمراهقين على التطبيقات الرقمية التي تسمح بحذف الرسائل والصور بعد ثوانٍ قليلة من عرضها، هو أنها تسمح بتجنب تلك الأوضاع. في المقابل، تنحو الصفحات القديمة على الـ «ويب» للبقاء، بطريقة أو أخرى. في 2010، جرى التنقيب على بروفایل الممثلة «أوكي كيوييد» العائد إلى مؤسس موقع «ويكيليكس» جوليان أسانج، ووضِع قيد النقاش العام⁽²⁵⁾.

لعل الأسوأ هم الناس الذين يستخدمون الإنترنت للتحرش والإذلال. تعطي «أشرطة الانتقام الإباحي» -والقسم الأكبر منها هو شاب ينشر صوراً عن ممارسة جنسية متفلنة مع صديقته السابقة- نموذجاً متطرفاً عن ذلك⁽²⁶⁾. جعلت مواقع نشر الصور التي تلتقطها الشرطة عند اعتقالها شخصاً ما، من ذلك المنحى تجارة كاملة قوامها الابتزاز⁽²⁷⁾. تعدُّ تلك الصور جزءاً من السجلات العامة، لكنها لا تكون متاحة بيسر. ويقتنص أصحاب مواقع «صور الاعتقال» كميات ضخمة منها، وينشرونها فيصبح بإمكان أي شخص الوصول إليها. وبعدها، يطلبون مالا ممن يرغب في إزالة صورته من تلك المواقع. إنه ابتزاز، على الرغم من كونه قانونياً بالمعنى التقني. لن تختفي تلك الأشياء، على الرغم من أن القانون ربما حظر أحياناً بعضاً منها.

نحتاج إلى التفكير بتلك الأمور. يستطيع كل شخص أن يشتري إحدى الأدوات المتقدمة في الرقابة، ما يعني أننا نحتاج إلى أعراف اجتماعية بصدد استعمالها أو عدمه. يعرف كل منا عن الآخر بأكثر مما نرتاح له، لذا يجب تطوير أعراف اجتماعية بصدد الإقرار بما نعرفه أو التظاهر بأننا لا نعرف. سعى ديفيد برين أساساً إلى إثارة تلك النقطة الأساسية في كتابه المجتمع الشفاف (Transparent Society)؛ بمعنى أن الرقابة الكلية القدرة آتية، وعلينا التكيف معها⁽²⁸⁾.

جسدت الإنترنت الفجوة الأضخم بين الأجيال، منذ عهد موسيقى الـ «روك أند رول» في أوساط الخمسينيات من القرن العشرين. ووفق ما أشار إليه كلاي شيركي، لم يكن الأكبر سنّاً مخطئين بشأن التغييرات كافة التي توقعوا أن تحدثها الـ «روك أند رول»، بل كانوا مخطئين بشأن مدى أذيتها⁽²⁹⁾. يتأقلم البشر. عندما تخلف الأفكار الشخصية لكل شخص منذ ولادته أثراً رقمياً عاماً، لن يفكر أي شخص مرتين بشأن وجودها. إذا كانت التكنولوجيا تعني أن كل ما نقوله -كل تلك الاتهامات المؤسفة، والتفاهات كلها معاً- سيسجل ويخزن إلى الأبد، يغدو واجباً علينا أن نتعلم كيف نعيش معها.

تكمُن المشكلة في أننا بارعون جداً في التأقلم، على الأقل في المدى القريب. إذ إنّ الناس الذين يترعرعون في ظل وجود رقابة أكبر، يغدّون أكثر ارتياحاً حيالها⁽³⁰⁾. يرتاد بعضنا مدارس فيها آلات للتحقق إلكترونياً من بطاقات الهوية وأجهزة كشف المعادن⁽³¹⁾. يعمل بعضنا في مبانٍ تطلب تفحص الشارات الشخصية يومياً. ومن يسافرون جواً في الولايات المتحدة، باتوا معتادين على إجراءات التفتيش من قبل «أمن إدارة النقل». ولم يعد المتسوقون كافة يتفاجأون بأخبار السرقات الكبرى لبيانات بطاقات الائتمان. تلك هي الطُرق التي رَوّضنا بها أنفسنا على القبول بخصوصية أقل. وعلى غرار كثير من الحقوق الأساسية، تمثل الخصوصية أحد تلك الأشياء التي نلاحظها عندما نفقدها. إنّه لأمر مؤسف؛ لأنه بعد غيابها يصبح من الصعب استرجاعها.

يجب وقف الانحدار. أساساً، الجدل حول الخصوصية هو أخلاقي. إنّ الخصوصية شيء يجب أن نمتلكه، ليس لكونه مربحاً أو عملياً، بل لأنه أخلاقي. يجب إلقاء الرقابة العامة في مزبلة التاريخ، لتضاف إلى ممارسات كثيرة عدّها البشر ذات مرة أمراً طبيعياً، لكننا ننظر إليها كونياً باعتبارها بغیضة. إنّ الخصوصية حق من حقوق الإنسان⁽³²⁾. ليست تلك فكرة جديدة. إذ جرى الاعتراف بالخصوصية بوصفها حقاً أساسياً في «الإعلان العالمي لحقوق الإنسان» (1948)، و«الميثاق الأوروبي لحقوق الإنسان» (1970)⁽³³⁾.

توجد الخصوصية في دستور الولايات المتحدة، ليس بصورة صريحة، لكنها متضمنة في التعديلات 4 و5 و9 فيه⁽³⁴⁾. ومثلت الخصوصية جزءاً من «شرعة الحقوق الأساسية في الاتحاد الأوروبي» (2000)⁽³⁵⁾. في 2013، أقرّت الجمعية العامة للأمم المتحدة قراراً عنوانه «الحق في الخصوصية في العصر الرقمي»، الذي شدّد على تطبيق الحق الأساسي في الخصوصية على شبكة الإنترنت وخارجها، وأنّ خطر الرقابة العامة ينسف ذلك الحق⁽³⁶⁾.

"شرعة الحقوق الأساسية في الاتحاد الأوروبي" (2000)⁽³⁷⁾

البند 7. احترام الحياة الشخصية والعائلية. لكل شخص الحق في أن تحترم حياته/حياتها الشخصية والعائلية، وكذلك المنزل والاتصالات.

البند 8. حماية البيانات الشخصية. 1 - لكل الحق في حماية البيانات الشخصية المتعلقة به/ بها. 2 - يجب التعامل مع تلك البيانات بطريقة عادلة تخدم غايات محدّدة، استناداً إلى موافقة الشخص المعني بها، أو أسس شرعية أخرى يقرّها القانون. 3 - يجب أن يوضع التحقق من إطاعة تلك القواعد، بيد سلطة مستقلة.

يُحتفى بتلك المبادئ في القانون وطنياً ودولياً. يجب علينا الشروع في اتباعها. ليست الخصوصية رفاهية يمكننا أن نحظى بها في أوقات الأمان وحدها. بالأحرى، إنها قيمة يجب حمايتها. إنها أمر أساسي للحرية والاستقلالية والكرامة الإنسانية. يجب أن نفهم أن الخصوصية ليست أمراً قابلاً لأن نتخلّص منه في سياق محاولة مذعورة لضمان الأمن، بل إنها شيء يجب صيانتها وحمايته من أجل الحصول على أمن حقيقي⁽³⁸⁾.

لن يحصل شيء من ذلك من دون تغيير التوجّه. في خاتمة المطاف، سنحصل على الخصوصية التي نطالب بها نحن كمجتمع، وليس أكثر من ذلك بقلامه ظفر.

لا تنتظر. كلما أطلنا انتظار التغيير، صار أمره أشد صعوبة. من ناحية الشركات، باتت ممارسة الرقابة الشاملة والإعلانات المشخصة عرفاً سارياً، وتحوز الشركات مجموعات ضغط سياسية تتكفل بتبديد محاولات التغيير.

يقدم «قانون كاليفورنيا لعدم التتبع» مثلاً عن ذلك. إذ ابتدأ كفكرة حسنة، لكنه بات منزوع الأنثاب كلياً عند إقراره. يتكفل المسار الطبيعي لتقنية الرقابة (أندكر الحديث عن انخفاض تكلفة الرقابة في الفصل 2؟)، وإرساء أمر واقع جديد، بجعل النجاح في إحداث التغييرات أمراً أكثر صعوبة في المستقبل، خصوصاً في الولايات المتحدة.

ليست الشركات وحدها من يقاوم التغيير. إذ يرغب السياسيون في البيانات عينها التي يسعى إليها المعلنون، وهي: البيانات الديموغرافية، والمعلومات عن التفضيلات الفردية للمستهلك، والمعتقدات الدينية والسياسية. إنهم يستخدمونها في حملاتهم، ولن يتخلّوا عنها. من الصعب تماماً إقناعهم بالتخلي عن الوصول إلى معلومات تساعدهم في بث رسائل موجهة، وحملات كشف التصويت وغيرها. وبمجرد أن يتوصّل أحدهم إلى فهم كيفية الاستفادة من تلك البيانات في جعل الانتخابات غير عادلة بصورة دائمة، على غرار ما يحصل عند التلاعب في التقسيم الإداري للمقاطعات لضمان ربح حزب معين؛ يغدو من الصعوبة بمكان إحداث التغيير.

في مؤتمر حضرته في 2014، تناهى إلى سمعي قول أحدهم: «إنّ قسم التحليلات» في محرك «غوغل» هو كوكابين من نوع الـ «كراك»، لرقابة الإنترنت. ما أن ترى تلك البيانات مرةً، حتى تصبح غير قادر عن التوقف». بصورة أكثر عموميّة، تضحي البيانات هي مبرّر نفسها بحد ذاتها. كلما أطلنا الانتظار، تصبح أعداد متزايدة من الناس والمؤسسات معتادة على الوصول الواسع لبياناتنا، ويزيد أيضاً ميلها للقتال دفاعاً عن ذلك الوصول.

نحن في وقت ملائم على نحو فريد، كي نُحدث تغييرات من الأنواع التي أوصيت بها في هذا الكتاب.

إن المؤسسات التي تجمع بياناتنا وتتاجر بها قويّة، لكنها حديثة العهد نسبياً. كلما نضجت وصارت أشد رسوخاً، سيغدو إحداث تغيير في طريقة عملها أشد صعوبة. وضع سنودن الرقابة الحكومية تحت ضوء كاشف بإظهاره أفعال «وكالة الأمن القومي» و«قيادة الاتصالات الحكومية». أدى ذلك إلى تنازع دولي فريد من نوعه، خصوصاً بين ألمانيا والولايات المتحدة. واخترق ذلك التوتر السياسي الانقسام الحزبي في الولايات المتحدة. يتيح ذلك الفرصة أمام تغيير حقيقي⁽³⁹⁾. ووفق كلمات

رام إيمانويل عمدة شيكاغو والرئيس السابق لموظفي أوباما: «لا تفوت فرصة حدوث أزمة فعلية»⁽⁴⁰⁾. ينطبق الأمر على هذا الوضع، على الرغم من أن معظم الناس لم يدرك أنها أزمة فعلية.

نحن في لحظة فريدة في العلاقة بين الولايات المتحدة والاتحاد الأوروبي. إذ يرغب الطرفان في تنسيق قوانينهما، وجعل التجارة بين حدودهما أكثر يسراً. من المحتمل أن تسير الأمور إلى أحد حدين: إما أن تضحي أوروبا أشد تساهلاً كي تتناغم مع الولايات المتحدة، أو أن تغدو الولايات المتحدة أكثر صرامة كي تتناغم مع أوروبا. وعندما ستساوى القوانين بين الطرفين، يصبح من الصعب تغييرها. نعيش أيضاً لحظة فارقة في تاريخ العصر الرقمي. إذ أدمجت الإنترنت في الأشياء كلها. نستطيع رؤية تلك النظم مرحلياً. بإمكاننا أن ندخل تغييرات عليها تستمر عقوداً.

حتى في تلك الحال، يجب أن نكون مستعدين لخوض ذلك كله كرة أخرى.

إذ تتغير التكنولوجيا باستمرار، ما يجعل أشياء جديدة ممكنة، فيما تغدو القوانين السابقة متقادمة. لا سبب يدعونا للتفكير بأن تقنيات الأمن والخصوصية وإغفال الهوية، وهي التي تحمينا ضد مخاطر اليوم، ستكون مجدية غداً.

تتغير الحقائق السياسية أيضاً، وتبدل القوانين معها. من الغباء التفكير بأنه إذا أرسينا مجموعة من الحلول اليوم، فلسوف تدوم إلى الأبد أو حتى إلى نصف قرن. يكفي إلقاء نظرة على التاريخ الأميركي الحديث لملاحظة أن الإساءات الكبرى لاستخدام السلطة التنفيذية - مع ما يرافقها من فضائح عامة كبرى وإصلاحات تخفيفية - تحدث كل 25 أو 30 سنة. من الأمثلة على ذلك «غارات بالمر»^(*) في

(*) بين خريف 1919 وشتاء 1920، شنت قوى الأمن بتفويض من المدعي العام ميتشيل بالمر، غارات على بيوت قادة النقابات العمالية والاشتراكيين وبعض الفوضويين، ورحلتهم قسراً عن الولايات المتحدة. ولاحقاً، صارت الغارات من رموز الاعتداء على الحريات والحقوق الأساسية للمواطن في أميركا.

عشرينيات القرن العشرين، والمكاثرة في خمسينيات القرن نفسه، وإساءة استعمال سلطة الـ «إف بي آي» و«وكالة الأمن القومي» في سبعينيات ذلك القرن أيضاً، والإساءات الجارية لاستخدام السلطة عقب 9/11 في مطلع القرن الجاري.

إذا أمعنت التفكير في الأمر، تمثل الثلاثون سنة متوسط مدة عمل الموظف المحترف في القطاع الحكومي. ويخامرني ظن بأن الأمر ليس مصادفة. ما يبدو أنه يجري هو أننا نحدث إصلاحات، ونتذكر لفترة لماذا أدخلناها، وفي النهاية يتغير عدد كاف من الناس في الحكومة، فنبداً بنسيان الأمر، ثم نعود كره ثانية إلى الإصلاحات ويجب علينا البدء بها مجدداً ضمن سياق تقني جديد.

سيتمتع على جيل آخر أن ينهض بالمحاسبة على المجموعة التالية من إساءة استخدام السلطة. وستكون تلك اللحظة لنا.

يتتابني قلق من أننا لسنا جاهزين تماماً. إنها مسألة تعاقب أجيال، ومنوط بالجيل التالي إحداث النقطات الاجتماعية اللازمة لتفعيل تغييرات سياسية تحمي خصوصيتنا الأساسية. أخشى أن الجيل الذي يتولى الأمور حاضراً مصاب بذعر فائض من الإرهابيين، ويتسرع في إعطاء الشركات كل ما ترغب به. أرجو أن أكون مخطئاً.

مقايضة «البيانات الضخمة»

تناول معظم هذا الكتاب سوء استعمال بياناتنا الشخصية ورداءته. في المقابل، لا بد من الإقرار بأن البيانات تملك قيمة لا تصدق في المجتمع.

تحوز بياناتنا قيمة كبرى عندما تُجمع معاً. إذ تساعد سجلات تحركاتنا في تخطيط الإعمار الحضري. وتمكّن سجلاتنا المالية الشرطة من اكتشاف الفساد وتبييض الأموال ومنعها أيضاً. وتساعد تدويناتنا وتغريداتنا البحثة في فهم ما يتفاعل في

المجتمع. هنالك كل أنواع الاستعمالات الإبداعية والمؤثرة لبياناتنا الشخصية، ويتولد منها معارف جديدة تحسّن حياتنا.

وكذلك تملك بياناتنا قيمة لكل منا إفرادياً، كي نُظهر منها أو نخفي ما نريد. وهنا تظهر العقدة. إذ يراهن استخدام البيانات على مصلحة المجموعة في مواجهة المصلحة الذاتية، وهو قلب تنازع ما فتأت الإنسانية تخوض فيه منذ وجودها الأول⁽⁴¹⁾.

لنتذكر الصفقات التي تحدّثت عنها في مقدّمة الكتاب. تمنحنا الحكومة صفقة: إذا أمتحت لنا الحصول على بياناتك كلّها، يمكننا أن نحميك من الجريمة والإرهاب. إنّها صفقة مخادعة، بل عديمة الجدوى أيضاً. إنّها تضخيم أمن المجموعة على حساب أمن الفرد.

يمنحنا «غوغل» صفقة مماثلة، وهي غير متوازنة على نحو مماثل: إذا أمتحت لنا الحصول على بياناتك كلّها وتخلّيت عن خصوصيتك، سنعرض عليك الإعلانات التي ترغب في رؤيتها، ونمنحك مجانية البحث على الإنترنت، والبريد الإلكتروني وأنواع الخدمات الأخرى كلّها. لا تتمكّن شركات كـ «غوغل» و«فيسبوك» من عرض تلك الصفقات، إلا إذا تخلّى عدد كبير منّا عن الخصوصية. إذاً، لا تستطيع المجموعة الاستفادة إلا إذا رضى عدد كبير من الأفراد.

لا تتسم بالقسوة كل تلك الصفقات التي تراهن على مصلحة المجموعة في مواجهة مصلحة الفرد. إذ يوشك المجتمع الطبي على عقد صفقة مماثلة معنا: دعنا نحصل على بياناتك الطيبة كافة، ولسوف نستخدمها في إحداث ثورة في الرعاية الصحية ونحسّن حياة كل فرد. في تلك الحال، أعتقد أنهم أحسنوا الصياغة. لا أعتقد أن كل شخص يستطيع فهم مدى استفادة الإنسانية من وضع بياناتنا الصحية كافة في قاعدة بيانات واحدة، وتمكين البّحاث من الوصول إليها⁽⁴²⁾. من المؤكّد أنّ تلك البيانات شخصية على نحو لا يصدّق، ومن المؤكّد أنها ستصل إلى أيادٍ

غير تلك التي قُصِدَ أن تكون بمتناولها، وتستعمل لغير الغاية منها. لكن في تلك الحال تحديداً، يبدو جلياً بالنسبة لي ضرورة تقديم مصلحة المجتمع في استعمال تلك البيانات. هناك كثيرون لا يوافقون على ذلك.

ثمة مثل آخر على التوازن الصحيح بين مصلحتي المجموعة والفرد. إذ حلل راينول جونكو، وهو باحث في شؤون الـ «سوشال ميديا»، عادات الدراسة بين طلبته⁽⁴³⁾. هناك كثير من الكتب على الإنترنت، وتجمع مواقع الكتب الشبكية كميات ضخمة من البيانات عن كيفية تفاعل الطلبة مع المواد الدراسية، وعدد المرات التي يفعلون بها ذلك. ودعم جونكو تلك المعلومات مع بيانات تأتت من رقابة النشاطات الحاسوبية الأخرى لطلبته. إنه ضرب من البحث المتعدي بطريقة لا تصدق، لكن مدته كانت محدودة، وأمدته بمعرفة جديدة عن طريقة دراسة الطالب الجيد والسيئ، كما طوّر تدخلات تهدف إلى تحسين عادات الدراسة عند الطلبة. هل فاقَت مصلحة المجموعة نظيرتها في الخصوصية بالنسبة لمن شاركوا في تلك الدراسة؟

وافق الطلبة على وضعهم تحت الرقابة، وحصل بحث جونكو على موافقة هيئة الأخلاق في الجامعة؛ ولكن، ماذا عن التجارب التي تجريها الشركات؟ لسنوات طويلة، دأب موقع «أو كي كيوييد» على إجراء تجارب على مستخدميه، مظهراً أو حاجباً صورهم على نحو انتقائي، مشدداً أو مخففاً من إجراءات التوافق مع شروط الموقع؛ وذلك ضمن سعيه لتفحص تأثير تلك المتغيرات في سلوك قاصدي الموقع⁽⁴⁴⁾. بإمكانك أن تحاجج بالقول إن تلك التجربة علمتنا الكثير، لكن من الصعوبة بمكان تبرير التلاعب بالناس بتلك الطريقة من دون معرفتهم ولا موافقتهم⁽⁴⁵⁾.

المرة تلو المرة، يظهر التنازع عينه: قيمة المجموعة في مواجهة قيمة الفرد. هناك قيمة لبياناتنا الجماعية في تقييم كفاءة البرامج الاجتماعية⁽⁴⁶⁾. هنالك قيمة لبياناتنا الجماعية بالنسبة لبحوث السوق. وتملك قيمة أيضاً في تحسين خدمات الحكومة.

هناك قيمة لدراسة الميول الاجتماعية، وتوقع الميول المستقبلية. يجب علينا الموازنة بين تلك المنافع من جهة، والمخاطر الناجمة عن الرقابة التي تمكن من الحصول على تلك البيانات.

يتمثل السؤال الكبير في التالي: كيف يمكننا تصميم نُظم تستطيع الاستفادة من بياناتنا الجماعية بصورة تفيد المجتمع ككل، مع حماية الناس إفرادياً في الوقت نفسه؟ وباقتباس صيغة من «نظرية الألعاب»^(*)، كيف نصل إلى «نقطة توازن ناش» في جمع البيانات، بمعنى إقامة توازن يفضي إلى محصلة نهائية مناسبة للجميع، حتى عندما نكف عن تكييف الأمور لأحد المكونات المفردة؟

ذلك هو الأمر. تلك هي القضية الرئيسة في عصر المعلومات. باستطاعتنا إيجاد حل لها، لكنها تتطلب تفكيراً متأنياً بشأن القضايا المحددة، وتحليلاً أخلاقياً عن تأثير الحلول المختلفة في قيمنا الأساسية.

قابلت بعضاً من النشطاء المتصلين بشأن الخصوصية الذين على الرغم من ذلك يفكرون بأنها ستكون جريمة ألا تضع بياناتك الطبية في قاعدة بيانات تشمل المجتمع الواسع. قابلت أناساً لا يعارضون الرقابة الأشد حميمية من الشركات، لكنهم يريدون ألا تلمس الحكومة تلك البيانات. قابلت أناساً لا يعارضون رقابة الحكومة، لكنهم يعترضون على أي شيء تحركه الرغبة في الربح. قابلت كثيرين من الناس ممن لا يعترضون على أي مما سبق ذكره.

كأفراد وكمجتمع، نحاول دوماً إقامة توازن بين قيمنا المختلفة. لا نتوصل إلى صيغة مثالية أبداً. لكن المهم هو أننا ننخرط بإرادتنا في تلك العملية. في أحيان كثيرة، يأتي التوازن لنا من الحكومات والشركات، وبواسطة أجدنتهم الخاصة.

أيّاً كانت سياساتنا، يجب أن نضع يدنا فيها⁽⁴⁷⁾. لا نريد أن تقرر الـ «إف بي آي» و«وكالة الأمن القومي» سراً، مستويات الرقابة الحكومية المتاحة بداهة على هواتفنا؛

(*) انظر ملاحظة في الفصل 13.

بل نريد من الكونغرس أن يقرّر أموراً كهذه وعبر نقاش عام ومفتوح. لا نريد أن تقرّر حكومات الصين وروسيا مستويات القدرة على الحجب في الإنترنت؛ بل أن يتقرر ذلك بواسطة هيئة ذات معايير دولية. لا نريد أن يقرر موقع «فيسبوك» مدى الخصوصية التي نتمتع بها مع أصدقائنا، بل نريد أن نقرر ذلك بأنفسنا. إنّ تلك القرارات كلها تفوق في حجمها وأهميتها أي منظمة مفردة. لذا، يجب أن تتقرر بواسطة مؤسسة كبرى تكون أكثر شمولاً وتمثيلاً. نريد أن يكون الناس قادرين على الخوض في نقاشات علنية عن تلك الأمور، وأن نكون «نحن الشعب» قادرين على محاسبة صنّاع القرار.

غالباً ما أستعيد عبارة للقس مارتن لوثر كينغ: «قوس التاريخ طويل، لكنه ينحني صوب العدالة»⁽⁴⁸⁾. أنا متفائل على المدى الطويل، حتى لو بقيت متشائماً على المدى القصير. أعتقد بأننا ستتغلب على خوفنا، ونتعلم كيف نعطي قيمة لخصوصيتنا، وأن نضع القانون في نصابه كي نحصد منافع «البيانات الضخمة»، مع الحفاظ على أمننا حيال بعض المخاطر. في اللحظة الراهنة، نحن نشهد بدايات حركة عالمية قوية لإقرار بالخصوصية كحق أساسي للإنسان، وليس بالمعنى المجرّد الذي رأيناه في إعلانات عامة كثيرة؛ بل بطريقة متمكنة ومحملة بالدلالات. يتولى الاتحاد الأوروبي القيادة، لكن آخرين يسرون معه. ستستغرق تلك العملية سنوات بل ربما عقوداً، لكنني أعتقد أنه بعد نصف قرن سوف ينظر الناس إلى الممارسات المعاصرة بشأن البيانات بالطريقة نفسها التي ننظر بها نحن الآن إلى ممارسات مهنية سابقة بوصفها بدائية ومهجورة، كالزراعة المأجورة وعماله الأطفال ونقابات التجّار في القرون الوسطى. تبدو تلك الأمور كلّها غير أخلاقية. إنّ نقطة البداية في تلك الحركة، أكثر من أي عنصر آخر، ستكون هي إرث إدوارد سنودن.

استهللت الكتاب بالحديث عن البيانات بوصفها «دخان العادم»، بمعنى أنها شيء ما تنتجه جميعاً أثناء نشاطاتنا في أعمال عصر المعلومات. وأعتقد أنني أستطيع السير بذلك التشبيه خطوة أبعد. إذ عدّ البيانات والمعلومات مشكلة التلوّث في

عصر المعلومات، وأن الخصوصية هي التحدي البيئي. تنتج معظم الكومبيوترات معلومات شخصية؛ وهي تلبث، وتتعمق. وتكون كيفية تعاملنا معها - كيف نحتويها وكيف نتخلص منها - قضية أساسية لصحة اقتصادنا المعلوماتي. ومثلما ننظر اليوم إلى العقود الأولى من الثورة الصناعية، ونتعجب من تجاهل أجدادنا للتلوث في خضم سعيهم المحموم لبناء عالم صناعي؛ كذلك سينظر أطفالنا خلفهم ليروا إلينا خلال العقود الأولى لعصر المعلومات، ويحاكمونا على طريقة تعاملنا مع تحدي جمع البيانات وإساءة استعمالها.

فلنحاول أن نجعلهم فخورين.

تنويهات

بالنسبة لي، يشكل تأليف كتاب خوضاً في غمار الاستكشاف. لا أعرف أين سأصل، إلى أن أنتهي من الكتابة. يجعل ذلك من الصعب عليّ تسويق الكتاب. إذ لا أكتب عرضاً عاماً له. وأكاد لا أستطيع القول بدقّة ما الذي يتناوله الكتاب. ولا يستسيغ الناشرون تلك الأمور.

أولاً: يجب عليّ أن أشكر وكيلي في النشر إريك نلسون من وكالة «سوزان رابينر ليتيرري إيجنسي»، الذي قدّم كتابي قبل أن يكون هناك كتاب. إذ اعتقد أنّه يستطيع تسويق «الكتاب التالي لشناير» للناشرين الرئيسيين، بل إنّهُ اعتقد بتلك الفكرة إلى حدّ أنّه لم يطلب توقيع عقد قبل بدئه بالعمل.

ثانياً: يجب عليّ أن أشكر ناشر كتابي، جيف شريفه، من «دار نورتون». إذ أبدى رغبته بشراء «الكتاب التالي لشناير» في ظل وجود توكيدات ضبابيّة عن موضوعه. كما أبدى قبوله بطريقتي في الكتابة.

لا أكتب الكتب من البداية إلى النهاية. بالأحرى أكتبها من تحت إلى فوق. أعني بذلك أنّه في كل لحظات الكتابة، أكون منغمساً في العمل على الكتاب برمته. يولّد ذلك أثرين غريبين: يتمثّل الأول في أنّ الكتاب يكون جاهزاً بمجرد شروعي في الكتابة. كل ما في الأمر أن الكتاب لا يكون في أفضل حال، لكنه يتحسن مع استمراره في الكتابة. ويتمثّل الأثر الثاني في أنني أستمر في كتابة الكتاب وتحسينه إلى الأبد، لو أتيح لي ذلك. جلّ ما أفعله هو أنني أحدّد بطريقة اعتباطيّة النقطة التي أقول فيها «انتهى»، عندما يدنو زمن تسليم الكتاب.

تتيح لي تلك الطريقة الحصول على آراء تقييمية أثناء عملية الكتابة. إذ قرأ كثيرون أجزاء من مسودة الكتاب أو طالعوها كلها، من بينهم: روس أندرسون، ستيف باس، كاسبر بويدن، كودي شاريت، ديفيد كامبل، كارين كوبر، دوروثي دينغ، كوري دوكتورو، ريان إليس، آديسون فيشر، كاميل فرانسوا، ناعومي غيلنز، جون غيلمور، جاك غولد سميث، بوب غورلاي، بيل هرذل، ديورا هورلاي، كريسا جاكسون، راينول يونكو، جون كلزاي، ألكسندر كليمبورغ، ديفيد ليفاري، ستيفن ليه، هاري لويس، يون لي، كين ليو، ألكس لوميس، ساشا ماينراث، إيشيا إم. ماكدونالد، بابلو مولينا، رامز نعام، بيتر نيومان، جوزيف ناي، كرستين باين، ديفيد م. بير، ليه بلونكت، ديفيد بريتنس، باراثا راغافان، مارك روتنبرغ، مارتن شنير، سيث ديفيد شيون، آدم شوستاك، بيتر سواير، كيت والش، سارة م. واتسون، ديفيد واينبرغر، داستن وينزل، مارسي ويلر، ريتشارد ويللي، بن ويزنر، جوزفين وولف، جوناثان زيتراين وشوشانا زوبوف. قدّم لي كل منهم اقتراحات أدبجتها في الكتاب.

كان لحفنة من الأشخاص مساهمة لا تقدر بثمن في وضع هذا الكتاب. وكانت كاثلين كايبل أفضل باحثة عرفتها على الإطلاق، وصرت غير قادر على تخيل تأليف كتاب من دون مساعدتها. ينطبق الأمر عيه على ربيكا كسلر التي حرّرت الكتاب مرتين أثناء عملية كتابته، وأعطتني اقتراحات نقدية في كل مرة. واستمر بيث فريدمان الذي تولى إعادة تحرير كل ما كتبه خلال السنوات العشر الأخيرة في إثبات أنه شخص لا غنى عنه.

أريد أن أتوجّه بالشكر أيضاً لإدوارد سنودن الذي أدت أفعاله الشجاعة إلى إثارة النقاش العالمي الذي انخرطنا فيه عن الرقابة. ليس مبالغة القول إنني لم أكن لأكتب هذا المؤلف لو لم يفعل سنودن ما فعله. وكذلك كان أمراً حسناً قراءة تلك الوثائق التي سرّ بها، خصوصاً أنني كنت مراقباً لأفعال «وكالة الأمن القومي» منذ سنوات طويلة.

ثمة ملاحظة بصدد العنوان. لقد أحببتُ وناشري عنوان المعلومات وجالوت بصورة فورية، لكن برزت مشكلة أيضاً. إذ نشر مالكوم غلادويل كتاباً بعنوان ديفيد وجالوت، قبل وقت قصير. لم يكن ذلك سيئاً تماماً، لكن كتابي السابق حمل عنوان كذبة ومرتدون، ونُشر مباشرة بعد صدور كتاب غلادويل عنوانه منشقون. وبدأ أمراً مفراطاً تقليدي لغلادويل مرتين. في نيسان (إبريل)، شرحتُ إشكاليتي تلك على مدوّنتي الإلكترونية. وفجأة، تلقيتُ رسالة إلكترونية من غلادويل تقول: «أحببتُ المعلومات وجالوت..». لذا، استندت إلى بركتة ودعابته، وأبقيتُ على العنوان.

كتبْتُ هذا المؤلّف أثناء فترة الزمالة في «معهد برلمان للإنترنت والمجتمع» في «كلية القانون» بـ «جامعة هارفرد»، ولا أستطيع أن أفي بالشكر لكل الأشخاص هناك. إذ ساعدني الوقت الذي قضيته مع زملائي وأساتذة «جامعة هارفرد» في التفكير بالقضايا التي أثارها في الكتاب؛ وكذلك الحال بالنسبة للطلبة في مجموعة القراءة التي توليت قيادتها في ربيع العام 2014. ومنذ كانون ثاني (يناير) 2014، توليت منصب «المدير الرئيس للتكنولوجيا» في شركة «ريزيليانت سيستمز» (Resilient Systems)، ويجب عليّ شكرهم أيضاً. وعلى رغم أن الكتاب لا يتصل مباشرة بما نقوم به في تلك الشركة، فإنهم أرخوا لي العنان كي أكتبه.

في الختام، أود أن أشكر أصدقائي، وخصوصاً زوجتي كارين كوبر، الذين تآزروا معي للوصول إلى مزاج «تأليف كتاب». أدرك جيداً أن الكتاب الحالي أكثر سهولة من الذي سبقه، لكنه كان صعباً أيضاً.

أشكركم جميعاً.

عن المؤلف

يحظى بروس شنابير بشهرة دولية عن كونه اختصاصياً تقنياً في الأمن، بل أطلقت عليه مجلة الإيكونوميست لقب «معلم الأمن». وضع شنابير 12 كتاباً من بينها كذبة ومتمردون: تفعيل الثقة التي يحتاجها المجتمع لينمو (2012)، إضافة إلى مئات المقالات والدراسات والأوراق الأكاديمية. ويتابع قرابة ربع مليون شخص نشرته الإخبارية «كريبتو- غرام» (Crypto-Gram) ومُدوّنته الإلكترونية «شنابير يتحدث عن الأمن» (Schneier on Security). ويتمتع شنابير بدرجة الزمالة من «مركز برلمان للمجتمع والإنترنت» (Berkman Center for Internet & Society) التابع لـ «كلية هارفرد للحقوق»، والزمالة في برنامج «المعهد المفتوح للتكنولوجيا في مؤسسة أميركا الجديدة» (New America Foundation's Open Technology Institute)، وهو عضو مجلس إدارة في «مؤسسة الحدود الإلكترونية» (Electronic Frontier Foundation)، وعضو المجلس الاستشاري في «مركز معلومات الخصوصية الإلكترونية» (Electronic Privacy Information Center). وكذلك يعمل مديراً في مؤسسة «ريزيلانتي سيستمز».

يمكن قراءة مدوّنته الإلكترونية ومقالاته وأوراقه الأكاديمية في موقع (schneier.com). ويمكن متابعة تغريداته في صفحته (@schneierblog).

كتب مختارة لبروس شناير

استمر: نصيحة صائبة من شناير حول الأمن (2013)

Carry On: Sound Advice from Schneier on Security (2013)

كذبة ومتمردون: تفعيل الثقة التي يحتاجها المجتمع لينمو (2012)

Liars and Outliers: Enabling the Trust That Society Needs to Thrive (2012)

شناير يتحدث عن الأمن (2008)

Schneier on Security (2008)

ما وراء الخوف: التفكير بمنطقية حول الأمن في عالم غير مستقر (2003)

Beyond Fear: Thinking Sensibly about Security in an Uncertain World (2003)

أسرار وأكاذيب: الأمن الرقمي في عالم تربطه الشبكات (2000)

Secrets and Lies: Digital Security in a Networked World (2000)

التشفير التطبيقي: بروتوكولات العمل، والخوارزميات، وشيفرة المصدر في

برنامج «سي» (1994 و1996)

Applied Cryptography: Protocols, Algorithms, and Source Code in C (1994 and 1996)

THE UNIVERSITY OF CHICAGO

THE UNIVERSITY OF CHICAGO

THE UNIVERSITY OF CHICAGO

THE UNIVERSITY OF CHICAGO

THE UNIVERSITY OF CHICAGO

THE UNIVERSITY OF CHICAGO

THE UNIVERSITY OF CHICAGO

THE UNIVERSITY OF CHICAGO

THE UNIVERSITY OF CHICAGO

THE UNIVERSITY OF CHICAGO

THE UNIVERSITY OF CHICAGO

THE UNIVERSITY OF CHICAGO

THE UNIVERSITY OF CHICAGO

THE UNIVERSITY OF CHICAGO

الهوامش

مدخل

1. ديفيد كرانندال وآخرون (8 ديسمبر 2010)، مقال: «استنتاج الروابط الاجتماعية من المصادفات الجغرافية». *Proceedings of the National Academy of Sciences of the United States of America* 107, <http://www.pnas.org/content/107/52/22436.short>
2. برهن السياسي الألماني مألته سبيتز عن قوة دمج بيانات المواقع الجغرافية بإعطائه معلومات عن إمكانية وجوده يومياً للصحافيين. مقال في «زايت أون لاين» (مارس 2011): «التليفون يخبر كل شيء». *Zeit Online*, (Mar 2011), «Tell-all telephone», *Zeit Online*, <http://www.zeit.de/datenschutz/malte-spitz-data-retention>
3. مانليو دي دومينيكو وأنطونيو ليما وميركو ميزوليبي (في 18 و 19 حزيران / يونيو 2012)، مقال: «الاعتماد المتبادل وتوقعية التحرك الإنساني والتفاعلات الاجتماعية». *Nokia Mobile Data Challenge Workshop, Newcastle, UK*, <http://www.cs.bham.ac.uk/research/projects/nsl/mobility-prediction>
4. التنسيق بين بيانات أبراج الخليوي وتسجيل المكالمات صوتياً على الأشرطة، يمثل دليلاً قوياً في المحاكم عن عدم مصداقية من يدافع عن نفسه؛ لأنها تبرهن كذبه بواسطة إظهار كلماته بالذات. شكل ذلك دليلاً في إدانة سكوت بيترسون في جريمة قتل زوجته في 2002؛ بعد أن تعاونت عشيقته أمير فرأي مع الشرطة. وكالة «أسوشيتد برس» في (27 آب / أغسطس 2004): «شهادة بيترسون تتحول إلى دليل إدانة في الحواسيب»، صحيفة يو إس داي تو داي
5. إيفان بيريس وسيوبهان غورمان (15 حزيران / يونيو 2013)، مقال في وول ستريت جورنال: «الهواتف تترك آثاراً دالة». *USA Today*, http://usatoday30.usatoday.com/news/nation/2004-08-27-peterson_x.htm
6. تريغور هيويز (7 كانون أول / ديسمبر 2013) مقال في «كولورادون»: «بيانات الهاتف تساعد في حل جريمتي مقاطعة لارمر». *Wall Street Journal*, <http://online.wsj.com/news/articles/SB10001424127887324049504578545352803220058>
7. تريغور هيويز (7 كانون أول / ديسمبر 2013) مقال في «كولورادون»: «بيانات الهاتف تساعد في حل جريمتي مقاطعة لارمر». *Coloradoan*, <http://archive.coloradoan.com/article/20131207/NEWS01/312070068/Cellphone-data-aided-solving-two-Larimer-County-murders>
8. تغالي الشرطة في دقة تلك المعلومات وتدين أبرياء بناءً على تلك البيانات. *الإيكونوميست* (6 أيلول / سبتمبر 2014)، مقال: «البرجان».
9. *Economist*,

<http://www.economist.com/news/united-states/21615622-junk-science-putting-innocent-people-jail-two-towers>.

مايك ماسينيك (9 أيلول/سبتمبر 2014) في «تيك ديرت»، مقال: «تبيّن أن البيانات المكانية للخلوية لا تقترب من الحقيقة، لكن الجميع مغرم بها».

Tech Dirt,

<https://www.techdirt.com/articles/20140908/04435128452/turns-out-cell-phone-location-data-is-not-even-close-to-accurate-everyone-falls-it.shtml>.

7. هيو موري (22 يناير 2014)، «زي ليد»، نيويورك تايمس، مقال: «رسائل نصية مشؤومة أرسلت إلى المحتجين في كيبك، تبعث الرعب في الإنترنت».

The Lede, New York Times,

<http://thelede.blogs.nytimes.com/2014/01/22/ominous-text-message-sent-to-protesters-in-kiev-sends-chills-around-the-internet>.

8. ميتشيل إيزيكوف (18 فبراير 2010)، مقال في نيوزويك: «الداف بي أي» يتتبع خلويات المشتبه فيهم، بلا مذكرات قضائية».

Newsweek,

<http://www.newsweek.com/fbi-tracks-suspects-cell-phones-without-warrant-75099>

9. ستيف أولاتسكي (17 يناير 2013)، مجلة فوريس، مقال: «هل يكون الإعلان الموجه وفق مكاناً هو مستقبل التسويق المتحرك والإعلان المتحرك؟»

Forbes,

<http://www.forbes.com/sites/marketshare/2013/01/17/is-location-based-advertising-the-future-of-mobile-marketing-and-mobile-advertising>.

جون ماكديرموت (20 فبراير 2014) في «ديجي داي»، مقال: «لماذا تلتهم الشركات الكبرى الإنترنت التطبيقات المستندة إلى تحديد المكان؟»

Digiday,

<http://digiday.com/platforms/apple-google-microsoft-yahoo-are-betting-on-mobile>

10. أنطون ترويانوفسكي (21 مايو 2013)، مقال في وول ستريت جورنال: «شركات الهاتف تباع بيانات المستهلكين».

Wall Street Journal,

<http://online.wsj.com/news/articles/SB10001424127887323463704578497153556847658>

راشيل كينغ (13 يوليو 2013)، وول ستريت جورنال بلوغز، مقال: «الخطر يتهدّد زبائن شركة «إيه تي أند تي» للهاتف».

CIO Journal, Wall Street Journal Blogs,

<http://blogs.wsj.com/cio/2013/07/13/aclu-att-customer-privacy-at-risk>

11. هياواثا براي (8 يوليو 2013)، واشنطن غلوب، مقال: «التنقيب في معلومات الخلوي لرسم بروفائلات شخصية».

Boston Globe,

<http://www.bostonglobe.com/business/2013/07/07/your-cellphone-yourself/eSvTK1UCqNOE7D4qbAcWPL/story.html>.

12. كريغ تيمبرغ (24 أغسطس 2014)، واشنطن بوست، مقال: «البيع: نُظُم تتبّع مستخدمي الخلوي أينما كانوا في الكرة الأرضية».

Washington Post,

http://www.washingtonpost.com/business/technology/for-sale-systemsthat-can-secretly-track-where-cellphone-users-go-around-the-globe/2014/08/24/f0700e8a-f003-11e3-bf76-447a5df6411f_story.html

13. «فرينت» (2014)
Verint (2014), «About Verint»,
<http://www.verint.com/about>.
14. «منظمة الخصوصية العالمية» (2012). «تبيع شركة «كوبهام» تقنيات مراكز للمراقبة، ورصد الهاتف، والرقابة التقنية والتتبع المكاني. لا يفرض قانون التوريد البريطاني قيوداً على تلك التقنيات، لذا فمن الممكن بسهولة أن تصل إلى أيدي غير مأمونة».
<https://www.privacyinternational.org/sii/cobham>.
15. ضمنت القائمة الكاملة في 2011: الجزائر، أستراليا، النمسا، بلجيكا، بروناي، جمهورية التشيك، جورجيا، غانا، إيرلندا، الكويت، ليبيا، النرويج، باكستان، السعودية، سنغافورة، جمهورية سلوفاكيا، إسبانيا، السويد، تايلاند، تركيا، المملكة المتحدة والولايات المتحدة.
- Cobham (2011), «Tactical C4I systems: Eagle—Close Combat Radio (CCR)»,
<https://s3.amazonaws.com/s3.documentcloud.org/documents/409237/115-cobham-tactical-c4i.pdf>
16. كريغ تيمبرغ (24 أغسطس 2014)، «واشنطن بوست»، مقال: «البيع: نظم تتبع مستخدمي الخليوي أينما كانوا في الكرة الأرضية».
Washington Post,
http://www.washingtonpost.com/business/technology/for-sale-systemsthat-can-secretly-track-where-cellphone-users-go-around-the-globe/2014/08/24/f0700e8a-f003-11e3-bf76-447a5df6411f_story.html
17. توبياس إنغل (9 يناير 2009)، «نادي فوضى الكمبيوتر»، مقال: «تحديد مواقع الخليويات باستخدام نظام الإشارة رقم 7».
Chaos Computer Club,
<http://berlin.ccc.de/~tobias/25c3-locating-mobile-phones.pdf>.
18. كيفن أوبراين (28 أكتوبر 2012)، «واشنطن بوست»، مقال: «المعلومات التي تجمعها التطبيقات تمثل مساحة رمادية قانونياً».
New York Times,
<http://www.nytimes.com/2012/10/29/technology/mobile-apps-have-a-ravenous-ability-to-collect-personal-data.html>
19. توجد مجموعة من التطبيقات المشابهة، ولكن يقدم «مالو سباي» مثلاً فاضحاً. وعلى الرغم من أن بيان رفع المسؤولية على الموقع الشبكي للتطبيق يورد أنه مصمم من أجل «التجسس الأخلاقي للأباء»، أو كي يستخدم في «هاتف نقال تملكه أو تملك موافقة ملائمة لرصده»، فإن النص نفسه يتفاخر بقدرته على العمل «في نسق شبكي»، كما يخصص صفحة للخيانة الزوجية.
<http://hellospy.com>.
20. إن «سبايس جيني» (SpaceGenie) هو تطبيق رقمي تجسسي آخر. في العام 2014، أدين مديره التنفيذي واعتُقل بتهمة بيعه في الولايات المتحدة. كريغ تيمبرغ ومات زاباتوسلي (29 سبتمبر 2014)، «واشنطن بوست»، مقال: «صانع سبايس جيني، وهو تطبيق تجسسي، يعتقل في فرجينيا».
Washington Post,
http://www.washingtonpost.com/business/technology/make-of-app-used-for-spying-indicted-in-virginia/2014/09/29/816b45b8-4805-11e4-a046-120a8a855cca_story.html
21. سبنسر آنغ ولورين ويبر (22 أكتوبر 2013)، «وول ستريت جورنال»، مقال: «ملاحظة إلى الموظفين: الرئيس يتجسس».
Wall Street Journal,
<http://online.wsj.com/news/articles/SB10001424052702303672404579151440488919138>

22. بارتون غيلمان وأشكان سلطاني (04 ديسمبر 2013)، واشنطن بوست، مقال: «وفق وثائق سنودن: وكالة الأمن القومي» تتتبع مواقع الخليويات في العالم».

WashingtonPost,

http://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html

بارتون غيلمان وأشكان سلطاني (10 ديسمبر 2013)، واشنطن بوست، مقال: «وثائق جديدة تكشف كيف تستنتج وكالة الأمن القومي» العلاقات بتحليل البيانات المكانية للخليوي».

Washington Post,

<http://www.washingtonpost.com/blogs/theswitch/wp/2013/12/10/new-documents-show-how-the-nsa-infers-relationships-based-on-mobile-location-data>

جيمس غلانز، وجيف لارسون وأندرو ديليو لهرن، (27 يناير 2014)، نيويورك تايمس، مقال: «وكالات الاستخبارات تسترق توجيه البيانات من تطبيق الخليوي».

New York Times,

<http://www.nytimes.com/2014/01/28/world/spy-agencies-scour-phone-apps-forpersonal-data.html>.

23. لا نعرف بصورة قاطعة إذا كانت تلك المعلومات صحيحة. دانا بريست (21 يوليو 2013)، واشنطن بوست، مقال: «تنغذى نمو وكالة الأمن القومي» من الحاجة لاستهداف إرهابيين».

Washington Post,

http://www.washingtonpost.com/world/national-security/nsagrowth-fueled-by-need-to-target-terrorists/2013/07/21/24c93cf4-f0b1-11e2-bed3-b9b6fe264871_story.html.

رايان غالاهاو (22 يوليو 2013)، موقع «سلايت»، مقال: «تقارير عن قدرة وكالة الأمن القومي» على تتبّع الخليويات حتى حين تكون مغلقة».

Slate,

http://www.slate.com/blogs/future_tense/2013/07/22/nsa_can_reportedly_track_cellphones_even_when_they_re_turned_off.html.

24. بمقدار ما أعرف، استخدم بيتر سواير ذلك المصطلح. بيتر سواير وكينزا أحمد (28 نوفمبر 2011). «مركز الديمقراطية والتكنولوجيا». مقال: «العصر الذهبي للرقابة مقابل التعقيم الشامل».

Center for Democracy and Technology,

<http://www.futureofprivacy.org/wp-content/uploads/Going-Dark-Versus-a-Golden-Age-for-Surveillance-Peter-Swire-and-Kenesa-A.pdf>.

25. بولي سبرنغر (26 يناير 1999)، مجلة وايرد، مقال: «شركة «صن» تتحدث عن الخصوصية: انس الأمر».

Wired,

<http://archive.wired.com/politics/law/new/1999/01/17538>

26. رئيس أركان الجيش الأمريكي (11 آب 2011)، بيان مشترك: «عمليات مشتركة».

Joint Publication 3-0,

http://fas.org/irp/doddir/dod/jp3_0.pdf.

27. إريك شميدت وإيارد كوهن (2013)، كتاب العصر الرقمي الجديد: إعادة رسم مستقبل الشعب والأهم والأعمال.

The New Digital Age: Reshaping the Future of People, Nations and Business, Knopf,

<http://www.newdigitalage.com>.

28. لم يشر أحد إلى الصفة، ولكن يردّد الجميع أنّ الرقابة ضرورية لحماية. باتريسيا زنفري وتبسم زكريا

(18 يونيو 2013)، مقال: «رئيس وكالة الأمن القومي»: المتحرّعون يدافعون عن برامج الرقابة»، «رويترز».

Reuters,

<http://www.reuters.com/article/2013/06/18/us-usa-security-idUSBRE95H15O20130618>.

تلفزيون «الجزيرة» (29 أكتوبر 2013): «رئيس وكالة الأمن القومي» يدافع عن برنامج التجسس بمواجهة

احتجاج من الحلفاء».

Al Jazeera,

<http://america.aljazeera.com/articles/2013/10/29/nsa-chief-defendsspyprogramamidusriftwitheurope.html>.

29. أثار يفتيني موروزوف، وهو من نقاد التكنولوجيا، تلك النقطة. يفتيني موروزوف، (22 أكتوبر 2013)، مجلة إم أي تي تكنولوجي ريفيو، مقال: «المشكلة الرقابة فعلياً».

MIT Technology Review,

<http://www.technologyreview.com/featuredstory/520426/the-real-privacy-problem>

الفصل 1: المعلومات منتجاً جانبياً للحوسبة

1. بيتر إيكسلي (يوليو 2010)، مقال: «ما مدى فائدة متصفحك للإنترنت؟» *Proceedings of the 10th International Conference on Privacy Enhancing Technologies*, Berlin, <https://panopticlick.eff.org/browser-uniqueness.pdf>.

2. بن فويديلا (21 فبراير 2012). مقال: «كيف يعمل: الكمبيوتر في سيارتك». *Popular Mechanics*, <http://www.popularmechanics.com/cars/how-to/repair/how-it-works-the-computer-inside-your-car>.

3. نايت كاردوزو (23 يوليو 2013). مقال في «مؤسسة الحدود الإلكترونية» بعنوان: «فرض صناديق سود في السيارات هو تعدُّ على الخصوصية».

Electronic Frontier Foundation,

<https://www.eff.org/press/releases/mandatory-black-boxes-cars-raise-privacy-questions>.

4. لوكاس مياريان (23 يوليو 2013). مقال في مجلة عالم الكمبيوتر بعنوان: «السيارة الذاتية القيادة تولد 01 غيغابايت من البيانات في الثانية».

Computer World,

http://www.computerworld.com/s/article/9240992/Self_driving_cars_could_create_1GB_of_data_a_second.

5. بنجامين هين، ماكسميليان كوخ وماثيو سميث. (3-7 مارس 2014)، ورقة بحثية بعنوان: «عن التوعية والسيطرة والخصوصية، بشأن «البيانات الوصفية» التي تحتويها الصور المتشاركة».

Distributed Computing & Security Group, Leibniz University, presented at the Eighteenth International Conference for Financial Cryptography and Data Security, Barbados,

http://ifca.ai/fc14/papers/fc14_submission_117.pdf.

6. الحال أن تلك القصة بالتحديد هي مريبة تماماً، بشأن الدسميتادات في الكاميرا. ماثيو هونان (19 يناير 2009)، مجلة وايرد، مقال بعنوان: «أنا هنا: قصة عن تجربة عيش رجل يعي أهمية بيانات المواقع».

Wired,

http://www.wired.com/gadgets/wireless/magazine/17-02/lp_guineapig.

7. باطارد، تعمل الحكومات على إزالة خيار الدفع نقداً المَغْفَل الهويّة. أدريان جفريس (27 مارس 2013)، مقال: «نظام الدفع غير النقدي عند «جسر البوابة الذهبية» يعد بالراحة مقابل الخصوصية».

Verge,

<http://www.theverge.com/2013/3/27/4150702/golden-gate-bridges-new-cashless-tollway-promises-convenience-for-privacy>.

أنه دو (20 مارس 2014)، صحيفة لوس أنجلوس تايمس، مقال: «العبور في شوارع مقاطعة «أورانج»

بأكية الدفع غير النقدي».

Los Angeles Times,

<http://www.latimes.com/local/lanow/la-me-ln-cashless-toll-roads-20140320-story.html>

تريغور بيتيفور (13 يونيو 2014)، مقال: «نظام عبور الشوارع في «فتيران» تصبح آلية الدفع».

Bay News 9,

http://www.baynews9.com/content/news/baynews9/news/article.html/content/news/articles/bn9/2014/6/13/veterans_expressway_.html.

مارتين باورز (17 يوليو 2014)، بوسطن غلوب، مقال: «بداية من الاثنين، لا دفع نقدي في بوابات شوارع «توبين»».

Boston Globe,

<http://www.bostonglobe.com/metro/2014/07/16/starting-monday-more-cash-tobin/WZKMDilsLULQrYiGZCrEK/story.html>.

8. «نست» (2014)، «آلة تنظيم حرارة «نست» قادرة على التعلم».

http://certified.nest.com/resources/NEST_POS_brochure_r7_300.pdf

9. إيزا باركلي (4 مايو 2012)، مقال: «الثلاجة الذكية تكتشف الخسة المفقودة، مقابل ثمن».

The Salt: What's On Your Plate, NPR,

<http://www.npr.org/blogs/thesalt/2012/05/03/151968878/the-smart-fridge-finds-the-lost-lettuce-for-a-price>.

10. راي كريست (8 يونيو 2014)، مقال: «مكيف الهواء الذكي من «هاير» أولاً في كونه مجازاً من «آبل» بين أنواع التجهيزات المنزلية».

CNET,

http://ces.cnet.com/8301-35306_1-57616915/haiers-new-air-conditioner-is-the-first-apple-certified-home-appliance

11. هيثر كيلي (15 يناير 2014)، مقال: «يرغب «غوغل» في السيطرة على منزلك بواسطة شركة «نست»».

شبكة «سي أن أن».

CNN,

<http://www.cnn.com/2014/01/15/tech/innovation/google-connect-home-nest>.

12. «وزارة الطاقة الأمريكية». دراسة: «مدخل إلى شبكات الكهرباء الذكية». (2008).

[http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/DOE_SG_Book_Single_Pages\(1\).pdf](http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/DOE_SG_Book_Single_Pages(1).pdf).

US Department of Energy (2014)، «What is the smart

grid?»، https://www.smartgrid.gov/the_smart_grid.

13. غريغوري فريشتاين. مقال: «كيف تستطيع آلات تتبّع المؤشرات الصحية خفض الخيانة الزوجية».

Tech Crunch,

<http://techcrunch.com/2013/07/05/how-health-trackers-could-reduce-sexual-infidelity>

14. قاعدة بيانات «فت بيت» (3 ديسمبر 2013).

Privacy policy,

<http://www.fitabase.com/Privacy>.

15. سارة إي. نيدلمان (14 أغسطس 2012). «وول ستريت جورنال». مقال: «أدوات طبية جديدة وذكية».

Wall Street Journal,

<http://online.wsj.com/news/articles/SB1000087239639044318104577587141033340190>

16. سارة واطسون (10 أكتوبر 2013). مجلة وايرد. مقال: «الهواتف الذكية الأكثر حداثة تستطيع أن تحولنا جميعاً أدوات لتتبع النشاطات».

Wired,

<http://www.wired.com/2013/10/the-trojan-horse-of-the-latest-iphone-with-the-m7-coprocessor-weall-become-qs-activity-trackers>.

17. توماس غويتز (17 نوفمبر 2007). مجلة وايرد مقال: «شركة 23 أند مي» ستفكك شيفرتك الوراثة لقاء 1000 دولار. أهلاً بكم في عصر المعلوماتية الجينية.

Wired,

http://www.wired.com/medtech/genetics/magazine/15-12/ff_genomics.

- إليزابيث مورفي (14 أكتوبر 2013). مقال: «جولة في أفكار مؤسسة 23 أند مي» أنا فويسكي عن ثورة الـ 99 دولاراً.

Fast Company,

<http://www.fastcompany.com/3018598/for-99-this-ceo-can-tell-you-whatmight-kill-you-inside-23andme-founder-anne-wojcickis-dna-r>.

18. تشارلز زايفه (27 نوفمبر 2013). مجلة ساينتيفك أميركان. مقال: «شركة 23 أند مي» مخيفة لأسباب غير التي يفكر فيها «مكتب الغذاء والدواء».

Scientific American,

<http://www.scientificamerican.com/article/23andme-is-terrifying-but-not-for-reasons-fda>

19. ربيكا غرينفيلد (25 نوفمبر 2013). مقال: «لماذا تخيف شركة 23 أند مي» شركات التأمين الصحي.

Fast Company,

<http://www.fastcompany.com/3022224/innovation-agents/why-23andme-terrifies-health-insurance-companies>.

20. ليو كيلبون (6 يناير 2014). «بي بي سي»، مقال: «سي إي أس»: شركة «سوني» تتباهى بتطبيق يشغل سجلاً للحياة.

BBC News,

<http://www.bbc.com/news/technology-25633647>

21. أليك ويلكنسون (28 مايو 2007). صحيفة نيويورك. مقال: «أندك ذلك؟ مشروع لتسجيل كل ما فعله في الحياة».

New Yorker,

http://www.newyorker.com/reporting/2007/05/28/070528fa_fact_wilkinson

22. جينا وورثام (8 مارس 2013). نيويورك تايمس بلوغز. مقال: «تعرف إلى «ميموتو» الكاميرا التي تسجل حياتك كلها».

New York Times Blogs,

<http://bits.blogs.nytimes.com/2013/03/08/meet-memoto-the-lifelogging-camera>

23. كين هيس (10 يناير 2014). مجلة زد دي نت. مقال: «نظرة إلى إنترنت الأشياء في 2014: كل الأشياء متصلة بالإنترنت وتتواصل مع بعضها بعضاً».

ZDNet,

<http://www.zdnet.com/the-internet-of-things-outlook-for-2014-everything-connected-and-communicating-7000024930>.

24. جورجينا ستاليويانو. (29 إبريل 2013). مقال: «الفكرة هي نشر مجسات لتراقب كل شيء في المدينة».

Press (Christchurch),

<http://www.stuff.co.nz/the-press/business/the-rebuild/8606956/Idea-to-have-sensors-track-everything-in-city>.

- فكتوريا تورك (يوليو 2013). مجلة وايرد. مقال: «مجسات المدن: إنترنت الأشياء تستولي على مدننا».

Wired,

<http://www.wired.co.uk/magazine/archive/2013/07/everything-is-connected/city-sensors>

25. سام بايفورد (5 يناير 2014). مقال: «فراشي أسنان ذكية» من شركة «كوليري» تزعم أنها تحسّن صحة الأسنان ونظافتها.

Verge,

<http://www.theverge.com/2014/1/5/5277426/kolibree-smart-toothbrush>

26. مارغريت رودس (23 سبتمبر 2014). مجلة وايرد. مقال: «مهندسون من الداناسا» وشركة «تسلا» يصنعون مصباح إنارة أكثر ذكاءً منك.

Wired,

<http://www.wired.com/2014/09/ex-tesla-nasa-engineers-make-light-bulb-thats-smarter>

27. ناقش تشارلز ستروس إملاءات تلك الأشياء. تشارلز ستروس (25 يونيو 2014). خطاب افتتاحي في جمعية مختصة في نيويورك عن «البرمجة في 2034».

Charlie's Diary,

<http://www.antipope.org/charlie/blog-static/2014/06/yapcna-2014-keynote-programmin.html>

28. فالنتينا بالادينو (8 يناير 2014). مقال: «زجاجة دواء ذكية من شركة «أدهير تيك» تعرف متى أخذت دواءك، ومتى لم تفعل».

Verge,

<http://www.theverge.com/2014/1/8/5289022/adheretech-smart-pill-bottle>

29. موقع «إيكونوكوم» (19 سبتمبر 2013). مقال: «عندما تتلاقى الموضة مع إنترنت الأشياء».

emedias,

<http://blog.econocom.com/en/blog/when-fashion-meets-the-internet-of-things>

30. لقد رأينا ذلك من قبل. إذ راجت الساعات الرقمية في سبعينيات القرن العشرين. في البداية، كانت تلك أدوات مستقلة بحد ذاتها- تضم منبهات وساعات-، ثم انخفض ثمنها. وصارت منبئة في أشياء أخرى كفرن الدمايكرويف، وسخان القهوة، والفرن المنزلي، ومنظم الحرارة، وجهاز الفيديو والتلفزيون. وتسير المجسات المتصلة بالإنترنت في الاتجاه عينه.

31. ناتاشا لوماس (9 مايو 2013). مقال: «مجسات «10 بي إن+» متصلة سلكياً بالأشياء حاضراً، ومجسات «30 بي إن+» ستكون متصلة بالإنترنت الأشياء في عشرينيات القرن الجاري؛ وفق بحث مؤسسة «إيه بي آي».

Tech Crunch,

<http://techcrunch.com/2013/05/09/internet-of-everything>

32. فالنتينا بالادينو (10 يناير 2014). مقال: «الذكاء الخفي: كيف تستطيع المجسات الدقيقة ربط كل الأشياء التي نملكها».

Verge,

<http://www.theverge.com/2014/1/10/5293778/invisible-intelligence-tiny-sensors-that-connect-everything>

33. بن هامرسل (يوليو 2013). مجلة وايرد. مقال: «عندما يصبح العالم هو الدويب».

<http://www.wired.co.uk/magazine/archive/2013/07/everything-is-connected/when-the-world-becomes-the-web>

34. وضع مطار «نيويورك» تلك الإشارات. ديان كارديول (17 فبراير 2014). صحيفة نيويورك تايمس. مقال: «إشارات السير في مطار «نيويورك» تعمل. إنها تراقبك».

New York Times,

<http://www.nytimes.com/2014/02/18/business/at-newarkairport-the-lights-are-on-and-theyre-watching-you.html>

35. أولغا كاريف (31 أكتوبر 2013). صحيفة واشنطن بوست. مقال: «مع انتقال الدرون» من القطاع العسكري إلى المدني، المستثمرون يتدخلون».

Washington Post,

http://www.washingtonpost.com/business/as-drones-evolve-from-military-to-civilian-uses-venture-capitalists-move-in/2013/10/31/592ca862-419e-11e3-8b74-d89d714ca4dd_story.html

36. بول ماكليري (29 يونيو 2014). مقال: «رادار قوي في منطاد، يراقب واشنطن (بليتمور) وصولاً إلى البحر». *Defense News*, <http://www.defensenews.com/article/20140629/DEFREG02/306290012/Powerful-Radar-Blimp-Surveil-Washington-Baltimore-Out-Sea>.
37. هناك الكثير من النقاش عن ذلك. «مؤسسة الحدود الإلكترونية» (2014). مقال: «تلاعب الحكومة بالكلمات عند الحديث عن «وكالة الأمن القومي» والتجسس الداخلي». <https://www.eff.org/nsa-spying/wordgames>
38. يستند ذلك إلى تقدير منطقي بأن الصفحة المكتوبة تحتوي 2 كيلوبايت. وعلى الرغم من ذلك، لا يكون التقدير كاملاً؛ لأن معظم ذلك المحتوى هو ملفات للصوت والصورة وأشرطة الفيديو.
39. إم. جي. سيفلر (4 أغسطس 2010). مقال: «إريك شميدت: في كل يوم، ننتج من المعلومات يمثل ما فعلنا منذ 2003». *Tech Crunch*, <http://techcrunch.com/2010/08/04/schmidt-data>
40. شركة «سيسكو» (10 يونيو 2014). «مؤشر «سيسكو» عن التشبيك البصري: المنهجية والتوقعات، 2013 - 2018». http://www.cisco.com/c/en/us/solutions/collateral/service-provider/ip-ngn-ip-next-generation-network/white_paper_c11-481360.html.
41. كريس إيفانز (18 إبريل 2014). مقال: «سلسلة الدأى إيه إيه أس»: تسعير التخزين في السحب الرقمية: ما هو أدنى سعر ممكن؟». *Architecting IT*, <http://blog.architecting.it/2014/04/18/iaas-series-cloud-storage-pricing-how-low-can-they-go>
42. ك. يونغ (6 سبتمبر 2012). مقال: «ما هي تكلفة تخزين كل التغريدات العابرة في الخطوط؟». *Mortar: Data Science at Scale*, <http://blog.mortardata.com/post/31027073689/how-much-would-it-cost-to-store-the-entire-twitter>.
43. بروسر كاamil (2013)، «تكلفة تخزين المكالمات الصوتية كافة لهواتف الولايات المتحدة في السنة، ما يتيح التنقيب على البيانات فيها». <https://docs.google.com/spreadsheets/cc?key=0AuqlWHQKl0oOdGJrSzhBVnh0WGlzWHpCZFNvURkXOE#gid=0>.
- في العام 2013، أنهت «وكالة الأمن القومي». جيمس بمفورد (15 مارس 2012). مجلة وايرد. مقال: «شيدت «وكالة الأمن القومي» أضخم مركز تجسس (راقب كلامك)». *Wired*, http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/all
44. مجلة فوربس (19 أكتوبر 2012). مقال: «مراكز المعلومات الخمسة الأضخم في العالم». *Forbes*, <http://www.forbes.com/pictures/fhgl45ijg/range-international-information-hub>
45. كشمير هيل (24 يوليو 2013). مجلة فوربس. مقال: «مؤشرات موثوقة عن «مركز يوتا للمعلومات» الذي بنته «وكالة الأمن القومي» بذخ صغير، تدل إلى أنه أقل قدرة على تخزين البيانات». *Forbes*, <http://www.forbes.com/sites/kashmirhill/2013/07/24/blueprints-of-nsa-data-center-in-utah-suggest-its-storage-capacity-is-less-impressive-than-thought>.
46. سيوبهان غورمان (21 أكتوبر 2013). صحيفة وول ستريت جورنال. مقال: «المقاولون يتقاتلون حول التأخر في إنجاز مركز بيانات لـ «وكالة الأمن القومي»». *Wall Street Journal*, <http://online.wsj.com/news/articles/SB10001424052702303672404579149902978119902>

47. راندال مونرو (2013). «مراكز البيانات في «غوغل» تعمل بالبطاقات المثقبة».
What If? XKCD,
<https://what-if.xkcd.com/63>
48. سايروس فاريفار (15 نوفمبر 2012). مقال: «كيف أرغم طالب قانون «فيسبوك» على الحذر بشأن الخصوصية».
Ars Technica,
<http://arstechnica.com/tech-policy/2012/11/how-one-law-student-is-making-facebook-get-serious-about-privacy>.
- أوليفيا سولون (28 ديسمبر 2012). هيئة الدبي بي سي. مقال: «كم يملك «فيسبوك» من المعلومات عن شخص واحد؟ 1200 صفحة من البيانات المتوزعة على 57 صنفاً».
BBC News,
<http://www.wired.co.uk/magazine/archive/2012/12/start/privacy-versus-facebook>
49. ما اكتشفه شريمز حفزه على رفع دعوى من الدرجة الأولى ضد «فيسبوك». ليات كلارك (01 أغسطس 2014). مجلة وايرد. مقال: «إصابة «فيسبوك» بدعوى قضائية عالمية».
Wired UK,
<http://www.wired.co.uk/news/archive/2014-08/01/facebook-class-action-lawsuit>

الفصل 2 : المعلومات بوصفها رقابة

1. ضمت صفوف من سربوا قبل سنودن وثائق عن الوكالة، توماس دريك، مارك كلاين وبيل بيني. لحد الآن، لم يجر التعرّف إلى مسربين بعد سنودن. بروس شناير (7 أغسطس 2014): «مجتمع الاستخبارات الأمريكي فيه مُسرب ثالث». كتاب شناير عن الأمن.
- Schneier on Security*,
https://www.schneier.com/blog/archives/2014/08/the_us_intellig.html
2. غلين غرينوالد (5 يونيو 2013). صحيفة الغارديان. «تجمع «وكالة الأمن القومي» سجلات هواتف الملايين من زبائن شركة «فريزون» يومياً».
- Guardian*,
<http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order>
3. باراك أوباما (7 يونيو 2013). «تصريح رئاسي».
 «Statement by the President,» US Executive Office of the President,
<http://www.whitehouse.gov/the-press-office/2013/06/07/statement-president>
- جيمس كلايدر (7 يونيو 2013) «بيان من «الاستخبارات الوطنية» عن الكشف غير المصرح به لوثائق سرية»، مكتب رئيس «الاستخبارات الوطنية».
- <http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/868-dni-statement-on-recent-unauthorized-disclosures-of-classified-information>.
- إد أوكيف (6 يونيو 2013)، صحيفة واشنطن بوست، مقال: «مقتطف: ديانا فاينشتاين، وفق شرح ساكسباي شامبلز، تدافع عن برنامج «وكالة الأمن القومي» في التجسس على الهواتف».
- Washington Post*,
<http://www.washingtonpost.com/blogs/post-politics/wp/2013/06/06/transcript-diannefeinstein-saxby-chambliss-explain-defend-nsa-phone-records-program>
4. هل أنا وحدي من يشتهي في سبب استعمال الرئيس أوباما كلمات محدّدة بعينها؟ إذ يقول دائماً أشياء كدائن أحداً لا يصني إلى مكالماتك الهاتفية». ويترك ذلك المجال مفتوحاً أمام إمكان أن تكون «وكالة الأمن القومي».

تعمل على تسجيل وتوثيق وتحليل مكالماتك - وربما أحياناً تستمع إليها. الأرجح أن ذلك صحيح، وهو شيء يتيح لرئيس بعقلية ضيقة أن يدعي لاحقاً بأنه لم يكن يكذب.

5. ثمة مقال جيد عن مدى حميمية الميتمادات، داليا ليتويك وستيف فلاديك (22 نوفمبر 2013)، مقال: «حذف ما لا أهمية له من البيانات الوصفية».

Slate,

http://www.slate.com/articles/news_and_politics/jurisprudence/2013/11/nsa_and_metadata_how_the_government_can_spy_on_your_health_political_beliefs.html

6. إدوارد دبليو فلتين (23 أغسطس 2013)، «إعلان من البروفسور إدوارد دبليو فلتين».

American Civil Liberties Union et al. v. James R. Clapper et al., United

States District Court, Southern District of New York (Case 1:13-cv-03994-WHP),

<https://www.aclu.org/files/pdfs/natsec/clapper/2013.08.26%20ACLU%20PI%20Brief%20-%20Declaration%20-%20Felten.pdf>

7. إيف- ألكسندر دي مونتجوي وآخرون (2-5 إبريل 2013). ورقة بحث عن «توقع شخصية الناس باستعمال طرق حسابية جديدة لتحليل بيانات الهواتف». قدمت في المؤتمر السادس عن الحوسبة الاجتماعية، النمذجة السلوكية- الثقافية والتوقع. واشنطن.

6th International Conference on Social Computing, Behavioral-Cultural Modeling and Prediction, Washington, D.C., <http://realitycommons.media.mit.edu/download.php?file=deMontjoye2013predicting-citation.pdf>.

8. تقدم شركة «أي بي أم» مستوى مرتفعاً في تحليل الميتمادات للهواتف. شركة «أي بي أم» (2014). «9 تي 225 ج: تحليل معلومات الهاتف باستخدام دليل «أي 2» للتحليل».

http://www.03.ibm.com/services/learning/content/ites.wss/zz/en?pageType=course_description&courseCode=9T225G&cc=.

9. جوناثان ماير وياتريك موتشر (14 مارس 2014). مقال: «ميثاقون: الطابع الحساس لمعلومات الميتمادات».

Web Policy, <http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata>

10. على الرغم من وضوح أنها بيانات وليس «بيانات وصفية»، يبدو أن «وكالة الأمن القومي» تعاملها كـ بيانات وصفية. واعتقد أن التبرير لذلك هو أن مفردات التفتيش تكون مشفرة في العنوان الإلكتروني للموقع. إذ إن الشرائح الضوئية لـ «وكالة الأمن القومي» تتحدث عن تجميع «عمليات التفتيش المستندة إلى الإنترنت»، مما يضيف وزناً إلى الاعتقاد بأن الوكالة تعاملها على أنها «ميتمادات» وليس معلومات. غلين غرينوالد (13 يوليو 2013). صحيفة الغارديان. مقال: «إكس كي سكور: وكالة الأمن القومي ترصد معظم ما يفعله مستخدم الإنترنت».

Guardian,

<http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data>

11. يثبت ذلك مجدداً أن الفارق قانونياً هو أقل من شعرة.

12. تكرر ذلك أيضاً مع عبارة: «هل يجب أن أخبر صديقتي؟»

13. أروى مهداوي (22 أكتوبر 2013). صحيفة الغارديان. مقال: «يكشف «غوغل» أفكارنا الأشد سوءاً».

<http://www.theguardian.com/commentisfree/2013/oct/22/google-autocomplete-un-women-ad-discrimination-algorithms>

14. دريك طومسون (1 نوفمبر 2010). مجلة أتلانتيك. مقال: «المدير التنفيذي لـ«غوغل»: القوانين تكتبها مجموعات الضغط».

Atlantic,

<http://www.theatlantic.com/technology/archive/2010/10/googles-ceo-the-laws-are-written-by-lobbyists/63908>.

15. بإمكانك التفتيش عن معلومات عن نمط النوم لدى أي مستخدم لـ«تويتر». أميت أغراوال (2013) «وقت النوم».

«Sleeping Time», *Digital Inspiration*,

<http://sleepingtime.org>.

16. هناك دراستان عن الرسوم البيانية للعلاقات الاجتماعية على «فيسبوك»، تظهر مدى سهولة كشف تلك الأمور. كارتر يارنغهام وبهرام ر. ت. ميسيري (5 أكتوبر 2009). دراسة: «اكتشاف المثليين بالحدس: «فيسبوك» يكشف توجهاتك الجنسية».

First Monday 14, <http://firstmonday.org/article/view/2611/2302>

مايكل كورنيسكي، ديفيد ستول، وثور غراييل (11 مارس 2013). دراسة: «الميل الشخصية والانتماءات قابلة للتوقع من السجلات الرقمية عن السلوك الإنساني».

Proceedings of the National Academy of Sciences of the United States of America (Early Edition),

<http://www.pnas.org/content/early/2013/03/06/1218772110.abstract>.

17. تستطيع أداة انغماسية صنعها «مختبر الميديا» في «معهد ماساشوستس للتقنية»، أن تصنع رسماً بيانياً اجتماعياً عنك، استناداً إلى «الدمياتادات» في بريدك الإلكتروني. «مختبر الميديا» (2013)، «انغماس: وجهة نظر مرتكزة إلى الناس في تحليل بريدك الإلكتروني».

<https://immersion.media.mit.edu>.

18. برايان لام (19 يونيو 2013). مجلة وايرد، مقال: «أوه... وكالة الأمن القومي» لا تجمع سوى «الدمياتادات»، لكن يجب أن تبقى قلناً».

Wired,

<http://www.wired.com/2013/06/phew-it-was-just-metadata-not-think-again>.

19. إدوارد دبليو فلتين (23 أغسطس 2013). «تصريح من البروفيسور إدوارد دبليو فلتين».

American Civil Liberties Union et al. v. James R. Clapper et al., United States District Court, Southern District of New York (Case 1:13-cv-03994- WHP),

<https://www.aclu.org/files/pdfs/natsec/clapper/2013.08.26%20ACLU%20PI%20Brief%20-%20Declaration%20-%20Felten.pdf>.

20. آلان روس بريدجر (21 نوفمبر 2013). نيويورك ريفيو أوف بوكس. مقال: «كشوفات سنودن وعامة الناس».

New York Review of Books,

<http://www.nybooks.com/articles/archives/2013/nov/21/snowden-leaks-and-public>

21. ديفيد كول (10 مايو 2014). مقال: «نقل الناس استناداً إلى معطيات «الدمياتادات»».

New York Review of Books,

<http://www.nybooks.com/blogs/nyrblog/2014/may/10/we-kill-people-based-metadata>.

22. جيم أو. كوملر. (1999). ستازي: القصة غير المعلنة للبوليس السري في ألمانيا الشرقية.

Westview Press,

<http://books.google.com/books?id=waxWwxY1tt8C>.

23. ماري دي روزا (2005). «البند 206: التوسع في التنصت تحت مظلة محكمة «قياس» ملخص».

Patriot Debates,

- http://apps.americanbar.org/natsecurity/patriotdebates/section-206
24. أثار ديفيد ليون تلك النقطة. ديفيد ليون (2003) «الرقابة بعد 9/11».
- Polity,
http://www.polity.co.uk/book.asp?ref=0745631819.
25. مجلة سكاي مول. «بريك هاوس سيكيوريتي» (2014). مقال: «أداة التجسس على «آي فون» / «أندرويد».
- Skymall,
https://www.skymall.com/iphone-%2F-android-spy-stick/28033GRP.html
26. «كي لوغرز. كوم» (2014). مقال: «أفضل مسجلات المفاتيح: مقارنة ومراجعة».
- http://www.keyloggers.com
27. «الجني الخفي» (2014). «اعتراض المكالمات الجارية».
- http://www.stealthgenie.com/features/live-call-intercept.html
28. موقع «أمازون. كوم» (2014). «دي جي أي فانتوم 2 مستعد لإطلاق هليكوبتر رباعية- مع «زيموز آتش 3 كاميرا ثنائية الأبعاد، «دغيمبال»: 959\$ (في القائمة 999\$)».
- Amazon.com,
http://www.amazon.com/Dji-Phantom-Ready-Fly-Quadcopter/dp/B00H7HPU54
29. هنالك نماذج أولية عن مجسات طائرة لها هيئة العصافير والحشرات، بل ربما أصغر- تقارب نثار الغبار- تحلق مع الريح. إليزابيث بوميلر وتوم شانكر (19 يونيو 2013). «صحيفة نيويورك تايمس، مقال: «الحرب تتطور مع الدرون، وأدوات تشبه الحشرات».
- New York Times,
http://www.nytimes.com/2011/06/20/world/20drones.html.
- جون دبلو وإتهيد (15 إبريل 2013). «صراصر ويعوض وعصافير: الثورة المقبلة في الدميرو- درون».
- Rutherford Institute,
https://www.rutherford.org/publications_resources/john_whiteheads_commentary/roaches_mosquitoes_and_birds_the_coming_micro_drone_revolution
30. أشكان سلطاني (9 يونيو 2014). مقال: «تكلفة الرقابة».
- http://ashkansoltani.org/2014/01/09/the-cost-of-surveillance
- كيفن إس. بانكستون وأشكان سلطاني (9 يناير 2014). «ضباط بأحجام ضئيلة وتكلفة الرقابة: مراكمة سنتات من المواجهة بين الولايات المتحدة والمجرمين المجهولين».
- Yale Law Journal 123,
http://yalelawjournal.org/forum/tiny-constables-and-the-cost-of-surveillance-making-cents-out-of-united-states-v-jones.
31. كاري جونسون (21 مارس 2012): «الهدف بي أي» تصارع قضائياً بشأن أحكام عن الدجي بي إس».
- NPR Morning Edition,
http://www.npr.org/2012/03/21/149011887/fbi-still-struggling-with-supreme-courts-gps-ruling
32. شون موسغريف (5 مارس 2014): «شبكة ضخمة للرقابة تجتاح أميركا بدفع من تجارة الامتلاك».
- BetaBoston/Boston
Globe, http://betaboston.com/news/2014/03/05/a-vast-hidden-surveillance-networkruns-across-america-powered-by-the-repo-industry
- شون موسغريف (5 مارس 2014): «قاعدة بيانات مكثفة عن اللوحات المعدنية للمركبات تشبه «إنستغرام»، وفق ما تشدد عليه «شبكة التعرف الإلكتروني».
- BetaBoston/Boston Globe,
http://betaboston.com/news/2014/03/05/massive-license-plate-location-database-just-like-instagram-digital-recognition-network-insists

33. «فيجيلانت فيديو» (23 فبراير 2009): «وثيقة إعدادية مختصة بالمواقع ومعدّة للتثبيت في خوادم «لين 4.0».

https://www.aclu.org/files/FilesPDFs/ALPR/texas/alprpra_portharthurPD_portarthurtx%20%287%29.pdf.

34. سايروس فاريفار (27 فبراير 2012): «سيارتك ملاحقة: الصعود السريع لظاهرة القارئات الضوئية للوحات المعدنية».

Ars Technica,

<http://arstechnica.com/tech-policy/2012/09/your-car-tracked-the-rapid-rise-of-license-plate-readers>

كاثرين كرامب (18 يوليو 2013). «الاتحاد الأمريكي للحريات المدنية»، «هناك من يتتبعك: كيف استخدمت القارئات الضوئية للوحات المعدنية في تعقب تحركات الأميركيين».

American Civil Liberties Union,

<https://www.aclu.org/files/assets/071613-aclu-alprreport-opt-v05.pdf>

35. كريغ تيمبرغ وإلين ناكاشيما (16 يونيو 2013). صحيفة واشنطن بوست. مقال: «قواعد بيانات صور بطاقات الهوية تحولت إلى كنوز للبوليس».

Washington Post,

www.washingtonpost.com/business/technology/state-photo-id-databases-become-troves-for-police/2013/06/16/6f014bd4-ced5-11e2-8845-d970ccb04497_story.html.

36. جوش هيكر (18 فبراير 2014). صحيفة واشنطن بوست. مقال: «وزارة الأمن الوطني تريد صنع قاعدة بيانات موحدة استناداً إلى القارئات الضوئية للوحات المعدنية للمركبات».

Washington Post,

<http://www.washingtonpost.com/blogs/federal-eye/wp/2014/02/18/homeland-securitywants-to-build-national-database-using-license-plate-scanners>.

دان فرومكين (17 مارس 2014) «تقارير عن موت قاعدة بيانات وطنية لتعقب اللوحات المعدنية».

Intercept,

<https://firstlook.org/theintercept/2014/03/17/1756license-plate-tracking-database>.

37. جيمس بريدل (18 ديسمبر 2013): «كيف استوردت المملكة المتحدة جيل المستقبل للرقابة».

Medium,

<https://medium.com/matter-archive/how-britain-exported-next-generation-surveillance-d15b5801b79e>.

جنيفر لينش وبيتر بيرنغ (6 مايو 2013). «مؤسسة الحدود الإلكترونية»، مقال: «القارئات الضوئية المؤتمتة للوحات المعدنية تهدد خصوصيتنا».

Electronic Frontier Foundation,

<https://www.eff.org/deeplinks/2013/05/alpr>.

38. تحصل الشرطة على تلك البيانات أيضاً. هيلين موهيلاند (2 أبريل 2012)، صحيفة الغارديان، مقال: «بوريس جونسون يخطط لنسخ الشرطة نفاذاً إلى كاميرات مراقبة المروء».

Guardian,

<http://www.theguardian.com/politics/2012/apr/02/boris-johnson-policecongestion-charge>.

39. دان فرومكين (17 مارس 2014): «مبالغة كبرى في التقارير عن موت قاعدة بيانات وطنية عن اللوحات المعدنية للمركبات».

Intercept,

<https://firstlook.org/theintercept/2014/03/17/1756license-plate-tracking-database>

40. مكتب الدواف بي أي، (15 سبتمبر 2014): «الدواف بي أي» تعلن امتلاك قدرة عملانية للجبل المقبل من نظام التعرف.
- <http://www.fbi.gov/news/pressrel/press-releases/fbi-announces-full-operational-capability-of-the-next-generation-identification-system>
41. وليم ماكلين (2 أكتوبر 2014). وكالة «رويترز». مقال: «مفتشو دبي يحصلون على نظارات «غوغل» لمكافحة الجريمة».
- Reuters,
<http://www.reuters.com/article/2014/10/02/us-emirates-dubai-google-police-idUSKCN0HR0W320141002>
42. غلين غرينوالد (5 يونيو 2013). صحيفة الغارديان، مقال: «تجمع «وكالة الأمن القومي» سجلات لملايين من زبائن «فريزون» يومياً».
- Guardian,
<http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order>
43. براندون كريغ (20 أغسطس 2013). شبكة «سي أن أن». «خرائط جديدة من «غوغل» تمكنك من تجنب ازدحام الطرق».
- CNN,
<http://www.cnn.com/2013/08/20/tech/mobile/google-waze-mobile-maps>
44. ألكساندرا ألتر (19 يوليو 2012). صحيفة وول ستريت جورنال. مقال: «قارتك الإلكتروني يقرؤك».
- Wall Street Journal,
<http://online.wsj.com/news/articles/SB10001424052702304870304577490950051438304>
45. ينطبق الوصف عيه على مشاهدتك لأشرطة الفيديو في «نتفلكس»، «أمازون»، «هولو» أو أي موقع لخدمة توجيه أشرطة الفيديو.
46. جنيفر لي (21 مارس 2002). صحيفة نيويورك تايمس. «نرحب بكم في ردهة قواعد البيانات».
- Jennifer 8. Lee (21 Mar 2002), «Welcome to the database lounge», *New York Times*,
<http://www.nytimes.com/2002/03/21/technology/welcome-to-the-database-lounge.html>
- Katie R. Holloman and D. Evan Ponder (2007), «Clubs, bars, and the driver's license scanning system», in *Privacy in a Transparent World*, ed. Amy Albert, Ethica Publishing,
<http://www.ethicapublishing.com/7CH5.htm>.
47. «بازفبيد» (10 إبريل 2014). «ما مدى حظوك الاجتماعية؟»
- <http://www.buzzfeed.com/regajha/how-privileged-are-you>
48. كايتلين ديوي (24 يونيو 2014). صحيفة واشنطن بوست. مقال: «الحقيقة المزعرة التي يجب أن تفتح العيون على التتبع في الإنترنت- عن الامتحانات القصيرة في موقع «بازفبيد» وغيره».
- Washington Post,
<http://www.washingtonpost.com/news/the-intersect/wp/2014/06/26/the-scary-eye-opening-truth-of-internet-tracking-on-buzzfeed-quizzesand-everywhere-else>
49. ماركو دي. هويشه (28 أكتوبر 2013): «تهديد الخصوصية أثناء البحث عن معلومات صحية».
- JAMA Internal Medicine,
<http://archinte.jamanetwork.com/article.aspx?articleid=1710119>
50. رون نيكسون (3 يوليو 2013). صحيفة نيويورك تايمس. مقال: «تقدّم «هيئة البريد في الولايات المتحدة» البريد كلّ إلى قوى إنفاذ القانون».
- New York Times,
<http://www.nytimes.com/2013/07/04/us/monitoring-of-snail-mail.html>

51. إم إس سميث (18 يونيو 2012). «نتورك وورلد». مقال: «مستقبل الرقابة بالدرون»: حشرة سايبورغية تكون «درون».

Network World,

<http://www.networkworld.com/article/2222611/microsoft-subnet/the-future-of-drone-surveillance--swarms-of-cyborg-insect-drones.html>.

52. رافي سوبان وبناتاترياي مانكايم (2014): «المؤشرات البيومترية في التعرف إلى الوجوه: تحليل ومراجعة». *Recent Advances in Intelligent Informatics: Advances in Intelligent Systems and Computing* 235,

http://link.springer.com/chapter/10.1007%2F978-3-319-01778-5_47

53. تشاو تشاو لو وإكزابو تانغ (15 إبريل 2014): «التفوق على القدرة البشرية في التأكد من الوجوه بواسطة الوجه المرسومة إحصائياً».

«Surpassing human-level face verification performance on LFW with GaussianFace», arXiv:1404.3840 [cs.CV],

<http://arxiv.org/abs/1404.3840>

54. باري فوكس (5 فبراير 2007). مجلة نيوساينتست. مقال: «ابتكار: جهاز خفي لمسح القرصنة». *New Scientist*,

<http://www.newscientist.com/article/dn11110-invention-covert-iris-scanner.html>

55. 133 زهاوزيانغ زانغ وماودي هو ويونغ هونغ وانغ. (2011). «مسح استقصائي عن التقدم في التعرف إلى طريقة المشي بالمؤشرات البيومترية».

Biometric Recognition, Lecture Notes in Computer Science 7098, Springer-Verlag, http://link.springer.com/chapter/10.1007%2F978-3-642-25449-9_19

56. كاثارين ألبريشت (2008). مجلة ساينتيفك أميركان (سبتمبر 2008)، مقال: «مؤشرات نظام «رفيد»: أنه هويتك».

72-77,

<http://www.scientificamerican.com/article/how-rfid-tags-could-be-used>.

University of Washington College of Engineering (22Feb 2008), «University launches RFID people tracking experiment», *RFID Journal*,

<http://www.rfidjournal.com/articles/view?6924>

كريستوفر زارا (8 يناير 2013). إنترناشيونال بيزنس تايمس، مقال: «سوار يعمل بنظام «رفيد» كأنه آت من عوالم «ديزني»، وهو يشكل منعرجاً خطراً وفق نشطاء الخصوصية».

International Business Times,

<http://www.ibtimes.com/disney-worlds-rfidtracking-bracelets-are-slippery-slope-warns-privacy-advocate-1001790>.

57. كوانتين هاردي (7 مارس 2013)، صحيفة نيويورك تايمس، مقال: «التقنية تركز على تعقب الناس خارج الإنترنت».

New York Times,

<http://bits.blogs.nytimes.com/2013/03/07/technology-turns-to-tracking-people-offline>.

58. ستيفاني كليفورد وكوانتين هاردي (15 يوليو 2013)، صحيفة نيويورك تايمس، مقال: «انتبهوا أيها المتبضعون: المخزن يتعقب هاتفكم الخليوي».

New York Times,

<http://www.nytimes.com/2013/07/15/business/attention-shopper-stores-are-tracking-your-cell.html>

برايدان فانغ (19 أكتوبر 2013). صحيفة واشنطن بوست. مقال: «كيف تستعمل المخازن الكبرى الدواء فاي» في هواتفكم كي تتعقب عاداتكم في التبضع».

Washington Post,

<http://www.washingtonpost.com/blogs/the-switch/wp/2013/10/19/how-stores-use-your-phones-wifi-to-track-your-shopping-habits>

لاتانيا سويني (12 فبراير 2014)، مقال: «هاتفك». «اللجنة الفيدرالية للتجارة في الولايات المتحدة».

<http://www.ftc.gov/news-events/blogs/techftc/2014/02/my-phone-your-service>

59. بران بون وآخرون (4-7 يونيو 2013)، «استعمال الإحصاء وموجات الدواي فاي» في التتبع اللاإرادي للناس أثناء المناسبات العامة.

14th International Symposium and Workshops on World of Wireless, Mobile and Multimedia Networks, Madrid,

<http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6583443>

60. كورت مغليبي (3 فبراير 2014)، «رسالة إلى المحترم آل فرانكين، مجلس الشيوخ الأمريكي»، طلب جواب بشأن تجميع المعلومات محلياً.

<http://www.franken.senate.gov/files/letter/140212FordResponse.pdf>

61. «مكتب موثوقية الحكومة» (6 ديسمبر 2013)، «خدمات مستندة إلى جمع بيانات من السيارات: الشركات تتخذ خطوات بشأن الخصوصية، لكن بعض المخاطر ليس واضحاً للزبائن»، تقرير إلى رئيس اللجنة الفرعية عن الخصوصية والتكنولوجيا والقانون، اللجنة التشريعية، مجلس الشيوخ.

GAO-14-81,

<http://www.gao.gov/products/GAO-14-81>

62. هيئة الدي بي بي سي (10 مارس 2008)، «كاميرا «تتظر» بواسطة الملابس».

BBC News,

<http://news.bbc.co.uk/2/hi/technology/7287135.stm>

روكو باراسكاندولا (23 يناير 2013)، صحيفة نيويورك تايمز، مقال: «مقوض قسم شرطة نيويورك يصرح بأن القسم يختبر قريباً أداة تقنية متقدمة جديدة تستطيع كشف الأسلحة المخبأة».

New York Daily News,

<http://www.nydailynews.com/new-york/nypdreadies-scan-and-frisk-article-1.1245663>

كارتر إم. أرمسترونغ (17 أغسطس 2012)، «الحقيقة حول رادار الدتيراهرتز».

IEEE Spectrum,

<http://spectrum.ieee.org/aerospace/military/the-truth-about-terahertz>

63. لاري هاردستي (4 أغسطس 2014)، «إم أي تي نيوز»، مقال: «استخراج الأصوات من البيانات البصرية».

MIT News,

<http://newsoffice.mit.edu/2014/algorithm-recovers-speech-from-vibrations-0804>

آبي ديفيس وآخرون (10-14 أغسطس 2014)، «الميكروفون البصري: الاستخراج السلبي للصوت بواسطة أشعة الفيديو».

41st International Conference on Computer Graphics and Interactive Techniques (SIGGRAPH 2014), Vancouver, British Columbia,

http://people.csail.mit.edu/mrub/papers/VisualMic_SIGGRAPH2014.pdf

64. إريك كين (30 ديسمبر 2013)، مجلة فوربس، مقال: «تقارير عن قدرة «وكالة الأمن القومي» على النفاذ إلى هواتف «آبل-آي فون»».

Forbes,

<http://www.forbes.com/sites/erikkain/2013/12/30/the-nsa-reportedly-has-total-access-to-your-iphone>

65. شاون ووترمان (9 مارس 2009)، وكالة أنباء «يو بي أي»، مقال: «وزارة الأمن الوطني تريد استعمار راحة الجسم البشري كمعزف بيوميتري ومؤشر للخداع».

UPI,

http://www.upi.com/Top_News/Special/2009/03/09/DHS-wants-to-use-human-body-odors-biometric-identifier-clue-to-deception/UPI-20121236627329.

66. براناف ديكيست (19 أغسطس 2014)، مجلة جزمودو، مقال: «البنوك باتت تتعرف إليك من طريقة طباعتك».

Gizmodo,

<http://gizmodo.com/your-phoncan-now-identify-you-based-on-how-you-type-1623733346>

67. يسمى ذلك «المؤثر الأسلوبى». ساديا أفروز وفريقها. (18-21 مايو 2014). ورقة بحث: «مكتشف الشبيه الشبحي: استعمال المؤثر الأسلوبى خفية».

IEEE Symposium on Security & Privacy, Oakland, California,

<http://www.cs.gmu.edu/~mccoy/papers/oakland2014-underground.pdf>.

68. رفايل ساتر (13 أكتوبر 2014). «وكالة أسوشيتدبرس». مقال: «حصد بصمات الصوت بالمالين».

Associated Press,

http://www.washingtonpost.com/business/technology/millions-of-voiceprints-quietly-being-harvested/2014/10/13/b34e291a-52af-11e4-b86d-184ac281388d_story.html

رفايل ساتر (13 أكتوبر 2014). «وكالة أسوشيتدبرس». مقال: «البنوك تحصد بصمات المكالمات بهدف مكافحة الفساد».

Associated Press,

http://www.washingtonpost.com/world/europe/banks-harvest-callers-voiceprints-to-fight-fraud/2014/10/13/715c6e56-52ad-11e4-b86d-184ac281388d_story.html.

69. نيكولا كلارك (17 مارس 2014). صحيفة نيويورك تايمس، مقال: «خطوط الطيران تستعمل التقنيات الرقمية كي تُضحي شخصية أكثر».

New York Times,

<http://www.nytimes.com/2014/03/18/business/airlines-use-digital-technology-to-get-even-more-personal.html>.

70. أندرو هوف (10 مارس 2010). صحيفة التلغراف، مقال: «[من وحي فيلم] تقرير الأقليات: لوحات الإعلان تراقب زبائن المحلات».

Telegraph,

<http://www.telegraph.co.uk/technology/news/7411249/Minority-Report-digital-billboard-watches-consumers-shop.html>.

71. كلينت بولدن (11 أكتوبر 2013)، صحيفة وول ستريت جورنال [بلوغز]، مقال: «صُناع أطعمة الدسناك» يحدّثون مستويات الشراء بواسطة المجسات وأدوات التحليل الرقمية».

Wall Street Journal Blogs,

<http://blogs.wsj.com/cio/2013/10/11/snackmaker-modernizes-the-impulse-buy-with-sensors-analytics>.

72. هناك فيلم خيال علمي يعرض تلك الأفكار بشكل ممتاز. كين ليو (ديسمبر 2012)، مجلة لايت سبيد، مقال: «التطابق الكامل».

Lightspeed Magazine,

<http://www.lightspeedmagazine.com/fiction/the-perfect-match>

73. برايان أكوهايدو (15 نوفمبر 2011)، صحيفة يو إس إيه توداي، مقال: «التدقيق في رقابة «فيسبوك»».

USA Today,

<http://usatoday30.usatoday.com/tech/news/story/2011-11-15/facebook-privacy-tracking-data/51225112/1>

74. كوتون ديلو (22 فبراير 2013): «شراكة «فيسبوك» مع شركة «أكزيكوم»، وشركة «إيبسلون» تقابل مشتريات المحلات مع بروفائيات مستخدميها».

Advertising Age,

<http://adage.com/article/digital/facebook-partner-axiom-epsilon-match-storepurchases-user-profiles/239967>

75. أحاول استخدام محرك البحث «داك داك غو» الذي لا يجمع بيانات شخصية عن مستخدميه.

<https://duckduckgo.com>.

76. جوناثان ماير (17 فبراير 2012)، ويب بوليسي، مقال: أدوات التعقب في محرك البحث «سفاري».

Web Policy,

<http://webpolicy.org/2012/02/17/safari-trackers>.

77. بنجامين ماكو هيل (11 مايو 2014). مقال: «يملك «غوغل» معظم بريدي لأنه يملك بريدك كله».

Copyrighteous,

<http://mako.cc/copyrighteous/google-has-most-of-my-email-because-it-has-all-of-yours>

78. مون مونغ (4 مايو 2011)، مقال: «المُن الخمسة الأولى في ضخامة الشبكات المخصصة لكاميرات المراقبة».

VinTech Journal,

<http://www.vintechology.com/journal/uncategorized/top-5-cities-with-the-largest-surveillance-camera-networks>

ديفيد باريت (10 يوليو 2013)، صحيفة التلغراف، مقال: «كاميرا مراقبة لكل 11 شخصاً شخص في لندن، وفق مسح إحصائي لـ«سي سي تي في».

Telegraph,

<http://www.telegraph.co.uk/technology/10172298/One-surveillance-camera-for-every-11-people-in-Britain-says-CCTV-survey.html>.

مجموعة «ثالث»، (11 إبريل 2014)، «مدينة مكسيكو بوصفها تمثل الطموح الأضخم لبرامج الأمن الحضري».

<https://www.thalesgroup.com/en/worldwide/security/case-study/mexico-city-worlds-most-ambitious-urban-security-programme>.

79. شركة «سي غايت تكنولوجيز» (2012)، «تخزين أشرطة الرقابة: ما هو الحد الكافي؟»

<http://m.seagate.com/files/staticfiles/docs/pdf/whitepaper/video-surv-storage-tp571-3-1202-us.pdf>

80. جبرمي بنثام (1791)، كتاب البان أوبتيكون أو منزل-التفتيش. دار النشر «تي. باين».

<http://cartome.org/panopticon2.htm>

81. أوسكار إتش غاندي جونيور (1993)، كتاب نوع البان أوبتيكون: الاقتصاد السياسي للمعلومات الشخصية، دار «ويست فيو برس».

<http://books.google.com/books?id=wreFAAAAMAAJ>.

82. توم برينغال الثالث (2002). كتاب: البان أوبتيكون الجديد: الإنترنت بوصفها بنية للسيطرة الاجتماعية. «جامعة تينيسي للتكنولوجيا».

<http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan003570.pdf>.

83. إلين ناكاشيما (16 يناير 2007). صحيفة واشنطن بوست. مقال: «التمتع بتسهيلات التكنولوجيا، مع عدم النجاة من رقابتها البقطة».

Washington Post,

<http://www.washingtonpost.com/wp-dyn/content/article/2007/01/15/AR2007011501304.html>

الفصل 3 : تحليل بياناتنا

1. تشارلز دو هيغ (16 فبراير 2012)، صحيفة نيويورك تايمز، مقال: «كيف تعرف الشركات أسرارك؟»
<http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html>.
2. غريغوري بياتسكي (8 ديسمبر 2013). مقال: «المراحل الثلاث للبيانات الضخمة».
KD Nuggets,
<http://www.kdnuggets.com/2013/12/3-stages-big-data.html>.
3. ميتشيل شراير (7 نوفمبر 2012)، مجلة تايم، مقال: «جولة في عالم ملتهمي المعلومات الذين ساعدوا في فوز أوباما».
Time,
<http://swampland.time.com/2012/11/07/inside-the-secret-world-of-quants-and-data-cruncherswho-helped-obama-win>
4. أقدم متلين عن ذلك. لارس باكستورم وآخرون (5 يناير 2012). «أربع درجات من الانفصال».
arXiv:1111.4570 [cs.SI],
<http://arxiv.org/abs/1111.4570>.
راسل ب. كلايتون (يوليو 2014). مقال: «الدولاب الثالث: أثر استخدام «تويتر» في الخيانة الزوجية والطلاق».
Cyberpsychology, Behavior, and Social Networking 17,
<http://www.cs.vu.nl/~eliens/sg/local/cyber/twitter-infidelity.pdf>.
5. تمكّنت تجربة من التمييز بين الرجال المثليين وغيرهم في 88 % من الحالات، وبين الأفارقة الأمريكيين ونظرائهم البيض في 95 % من الحالات، وبين الديمقراطيين والجمهوريين في 85 % من الحالات. ميشال كوزنسكي، ديفيد ستولويل، وثور غرايبل (11 مارس 2013)، دراسة: «الخصائص والانتماءات الشخصية قابلة للتوقع من السجلات الرقمية».
Proceedings of the National Academy of Sciences of the United States of America, Early Edition, <http://www.pnas.org/content/early/2013/03/06/1218772110>.
6. سارة م. واتسون (14 مارس 2012)، مجلة أتلانتيك، مقال: «لم أخبر «فيسبوك» بخطوبتي، فلماذا يسألني عن خطيبي؟»
Atlantic,
<http://www.theatlantic.com/technology/archive/2012/03/i-didnt-tell-facebook-im-engagedso-why-is-it-asking-about-my-fianc/254479>.
7. كاتي هايني (19 مارس 2013). مقال: «عرف «فيسبوك» أنني مثلي جنسياً قبل أن تعرف عائلتي بذلك».
BuzzFeed,
<http://www.buzzfeed.com/katieheaney/facebookknew-i-was-gay-before-my-family-did>
8. جيفري أ. فاوляр (13 أكتوبر 2012). صحيفة وول ستريت جورنال، مقال: «عندما يعلن «فيسبوك» على الملأ، الأسرار الأكثر حميمية».
Wall Street Journal,
<http://online.wsj.com/news/articles/SB10000872396390444165804578008740578200224>
9. في فترة ما من العام 2014، تضمّن تطبيق «غرندر» (Grindr) المخصّص للمثليين، معلومات تمكن من الوصول إلى كل مثلي جنسياً في العالم، بما في ذلك بلدان كأوغندا وروسيا وإيران. جون أرافوسس (26 أغسطس 2014)، مقال: «تطبيق «غرندر» الشائع بين مثليي الجنس يواجه اختراقات أمنية مريبة».
America Blog,
<http://americablog.com/2014/08/grindr-users-unwittingly-giving-away-exact-location.html>.
10. سارة م. واتسون (16 سبتمبر 2014). قناة «الجزيرة» وموقعها الإلكتروني. مقال: «أسأل جهاز فك تشفير قنوات التلفزيون: التريص بالضربات».

- Al-Jazeera,
<http://america.aljazeera.com/articles/2014/9/16/the-decoder-stalkedbysocks.html>
11. سيلفان لاين (13 أغسطس 2014). «الإعلانات الـ16 الأكثر إثارة للريبة على «فيسبوك»».
- Mashable,
<http://mashable.com/2014/08/13/facebook-ads-creepy>.
12. غاي غفليوتا (19 يونيو 2006). صحيفة واشنطن بوست. مقال: «التنقيب في البيانات ما زال بحاجة إلى توجيه ليكون فعالاً».
- Washington Post,
<http://www.washingtonpost.com/wp-dyn/content/article/2006/06/18/AR2006061800524.html>
فيليب سيفال (28 مارس 2011). مقال: «التنقيب في المعلومات ذكاء يسير بغباء».
- Ethical Investigator,
<http://www.ethicalinvestigator.com/internet/data-mining-is-dumbed-down-intelligence>.
أوغي أوغاس (8 فبراير 2013). مجلة وايرد، مقال: «احذر من الأخطاء الضخمة في البيانات الضخمة».
- Wired,
<http://www.wired.com/2013/02/big-data-means-big-errors-people>.
13. بارتون غيلمان وآشكان سلطاني (18 مارس 2014). صحيفة واشنطن بوست. «برنامج الرقابة في وكالة الأمن القومي» يصل إلى الماضي، ويستعيد المكالمات الهاتفية ويشغلها».
- Washington Post,
http://www.washingtonpost.com/world/national-security/nsa-surveillance-program-reaches-into-the-past-to-retrieve-replay-phone-calls/2014/03/18/226d2646-ade9-11e3-a49e-76adc9210f19_story.html.
14. وزارة العدل الأمريكية. (16 ديسمبر 2009). «وافق بنك «كريدو ليونيه» على دفع غرامة بـ536 مليون دولار تتعلق باختراجه «قانون الأحوال الطارئة لقوى المالية الدولية» وقانون مقاطعة نيويورك».
- <http://www.justice.gov/opa/pr/2009/December/09-ag-1358.html>.
مكتب المدعي العام لمقاطعة نيويورك (10 ديسمبر 2012). «بنك «ستاندرد شارتز» يقبل دفع 327 مليون دولار غرامة عن معاملات غير قانونية».
- <http://manhattanda.org/node/3440/print>
مكتب المدعي العام لمقاطعة نيويورك (30 حزيران 2014). «بنك «بي أن بي باري باه» يقر بأنه مذنب، ويقبل بدفع 8.83 بليون دولار غرامة عن معاملات غير قانونية».
- <http://manhattanda.org/node/4884/print>.
15. سكوت روزنفيلد (23 يوليو 2013). نتائج إيجابية [بوجود منشطات] لثلاثة من أوائل الدراجين في مسابقة «تور دي فرانس».
- Outside Online,
<http://www.outsideonline.com/news-from-the-field/Top-3-Finishers-in-1998-Tour-Test-Positive.html>
16. غلين غرينوالد (21 يوليو 2013). صحيفة الغارديان. مقال: «أداة «إكس كي سكور» لدى «وكالة الأمن القومي» تجمع معظم ما يفعله جمهور الإنترنت».
- Guardian,
<http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data>
«وكالة الأمن القومي» (8 يناير 2007) «إكس كي سكور» (شرائح ضوئية تدريبية).
<https://www.eff.org/document/2013-07-31-guard-xkeyscore-training-slides-page-2>.
17. جيمس بول (30 سبتمبر 2013)، صحيفة الغارديان، مقال: «قاعدة بيانات لدى «وكالة الأمن القومي» تحفظ بالـ «ميتاداتا» للذين مستخدمي الإنترنت لسنة، وفق ما تظهره ملفات سرية».

Guardian,

<http://www.theguardian.com/world/2013/sep/30/nsa-americans-metadata-year-documents>

18. ريان ديفيرو، غلين غرينوالد ولورا بيوتراس (19 مايو 2014). «قراصنة البيانات في الكاريبي: وكالة الأمن القومي» تسجل المكالمات الخلوية كافة في الدباهاماس.

Intercept,

<https://firstlook.org/theintercept/article/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas>

جوليان أسانج (23 مايو 2014)، «إعلان من «ويكيليكس» بصدد تسجيلات الهاتف الجماعية للأفغان، من قبل «وكالة الأمن القومي».

WikiLeaks,

<https://wikileaks.org/WikiLeaks-statement-on-the-mass.html>.

19. ديفيد كرافتس (17 يناير 2014)، مجلة وايرد، مقال: أوباما يعيد هيكلة برنامج «وكالة الأمن القومي» في التجسس على الديمقراطيات.

Wired,

<http://www.wired.com/2014/01/obama-nsa>.

20. لا أعرف إذا كان ذلك يشمل الحوارات الشبكية المشفرة بطريقة «إس إس إل»، لكن يخامرني ظن بأن الوكالة تفكك (تلك) كثيراً من ذلك التشفير في الوقت الحالي. ماثيو غرين، (2 ديسمبر 2013)، مدونة إلكترونية، كيف تكسر «وكالة الأمن القومي» شيفرة الدراس إس إل؟

A Few Thoughts on Cryptographic Engineering,

<http://blog.cryptographyengineering.com/2013/12/how-does-nsa-breakssl>.

21. بارتون غيلمان وآشكان سلطاني (4 ديسمبر 2013)، صحيفة واشنطن بوست. مقال: «تتعقب» وكالة الأمن القومي» الهواتف في العالم كله.

Washington Post,

http://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html

22. جيمس مامفورد (15 مارس 2012)، مجلة وايرد، مقال: «وكالة الأمن القومي» تبني المركز الأضخم للتجسس في البلاد (راقب ما تقوله).

Wired,

http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/all.

23. كيفن بولسن (27 يناير 2014)، مجلة وايرد، مقال: «إذا استخدمت هذا الموقع الآمن للبريد الإلكتروني، يحصل الدوافع بي أي» على رسائلك.

Wired,

<http://www.wired.com/2014/01/tormail>.

24. سايروس فاريفار (27 فبراير 2012)، مقال: «سيارتك ملاحقة: الصعود السريع لظاهرة الماسحات الضوئية للوحات المركبات». موقع «أرس تكنيكا».

Ars Technica,

<http://arstechnica.com/tech-policy/2012/09/your-car-tracked-the-rapid-rise-of-license-plate-readers>.

Steve Orr (26 Jul 2014), «New York knows where your license plate goes»

Democrat and Chronicle,

<http://www.democratandchronicle.com/story/news/2014/07/26/new-york-licenseplate-readers/13179727>.

25. ديكلان مانكوله (19 مارس 2013). مقال: «رجال شرطة يطلبون أن يتضمن قانون الولايات المتحدة ما يتيح الحصول على سجلاتك الهاتفية». موقع «سي نت» للأخبار.

CNET,

http://news.cnet.com/8301-13578_3-57575039-38/cops-u.s-law-should-require-logs-of-your-text-messages.

على بُعد ثلاث «قفزات» من أليس. فيليب بوم (17 يوليو 2013)، أتلانتك واير، مقال: «وكالة الأمن القومي تقر بأنها تحلل بيانات الناس بأكثر مما صرحت عنه سابقاً».

Atlantic Wire,

<http://www.thewire.com/politics/2013/07/nsa-admits-it-analyzes-more-peoples-data-previously-revealed/67287>.

26. يكتب جوناثان مايرز عن صعوبة تحليل تلك البيانات. جوناثان مايرز وياترك موشلر (9 ديسمبر 2013). الدميّاء هاتف: القفزات الثلاث لـوكالة الأمن القومي».

Web Policy,

<http://webpolicy.org/2013/12/09/metaphone-the-nsa-threehop>.

27. أمي دافيدسون (16 ديسمبر 2013). صحيفة نيويورك. نظرية الدومينو، افتراضياً: القاضي ليون في مواجهة «وكالة الأمن القومي».

New Yorker,

<http://www.newyorker.com/news/amy-davidson/the-dominos-hypothetical-judge-leon-vs-the-nsa>.

28. بارتون غيلمان ولورا بواتراس (10 يوليو 2013). صحيفة واشنطن بوست. مقال: «الشرائح الضوئية لـوكالة الأمن القومي» تشرح طريقة عمل برنامج «بريزم» لجمع البيانات».

Washington Post,

<http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents>

29. شاين هاريس (17 يوليو 2013). مجلة فورين بوليسي، مقال: ثلاث درجات من الانفصال تكفي لوضعك تحت رقابة «وكالة الأمن القومي».

Foreign Policy,

http://complex.foreignpolicy.com/posts/2013/07/17/3_degrees_of_separation_is_enough_to_have_you_watched_by_the_nsa.

30. طوني برادلي (17 يناير 2014). مجلة فوربس، مقال: «ما قاله الرئيس أوباما ولم ينفذه».

Forbes,

<http://www.forbes.com/sites/tonybradley/2014/01/17/nsa-reform-what-president-obama-said-and-whathe-didnt>.

31. جيمس ريزن ولورا بواتراس (20 سبتمبر 2013). صحيفة نيويورك تايمس، مقال: «وكالة الأمن القومي» تراقب العلاقات الاجتماعية للمواطنين الأميركيين».

New York Times,

<http://www.nytimes.com/2013/09/29/us/nsa-examines-social-networks-of-us-citizens.html>

32. فوهيني فارا (23 أغسطس 2007)، صحيفة وول ستريت جورنال، مقال: «الانتقال إلى الشخصن في إعلانات فيسبوك».

Wall Street Journal,

<http://online.wsj.com/news/articles/SB118783296519606151>

33. عندما تعثر «مايكروسوفت» أو «غوغل» على أدلة عن جنس أطفال إباحي، فإنها تبلغ الشرطة عنك. ماثيو سباركس (4 أغسطس 2014)، صحيفة التلغراف، مقال: «لماذا يذوق «غوغل» في بريدك بشأن جنس أطفال إباحي».

Telegraph,

<http://www.telegraph.co.uk/technology/google/11010182/Why-Google-scans-your-emails-forchild-porn.html>.

ليو كليون (6 أغسطس 2014). هيئة «بي بي سي»، مقال: «مؤشرات من «مايكروسوفت» أدت إلى اعتقالات في «بنسلفانيا» بشأن جنس أطفال إباحي».

BBC News,

www.bbc.co.uk/go/em/fr/-/news/technology-28682686

34. أشار «مجلس الإشراف على الخصوصية والحريات المدنية» إلى أن جميع «وكالة الأمن القومي» للبيانات تحت البند 702 من «قانون إصلاحات محكمة «فيسا»، لا ينطبق تجميع أسس الكلمات المفتاحية، على الرغم من كونه صلاحية منفردة، ما يعني وجود مساحة للتلاعب. «مجلس الإشراف على الخصوصية والحريات المدنية» (2 يوليو 2014).

«Report on the surveillance program operated pursuant to Section 702 of the Foreign Intelligence Surveillance Act.»

<http://www.pclob.gov/All%20Documents/Report%20on%20the%20Section%20702%20Program/PCLOB-Section-702-Report.pdf>.

جنيفر غرانيك (11 فبراير 2014)، «ثمانية أسئلة من «مجلس الإشراف على الخصوصية والحريات المدنية» بشأن البند 207».

Just Security,

<https://justsecurity.org/7001/questions-pclob-section-702>

35. جاكوب آبلوم (3 يوليو 2014). مقال: «وكالة الأمن القومي تستهدف الأشخاص المنتخبين للخصوصية».

Panorama,

http://daserste.ndr.de/panorama/aktuell/nsa230_page-1.html.

36. مارسي وييلر (15 نوفمبر 2013). موقع «إيمبتي وييل». مقال: «عن رأي محكمة «إف أي أس سي» في مايو 2007».

Empty Wheel,

<http://www.emptywheel.net/2013/10/15/aboutthat-may-2007-fisc-opinion>

37. مارسي وييلر (16 مايو 2014). موقع «إيمبتي وييل»، مقال: «عملية البحث المؤتمتة ستشمل روابط».

Empty Wheel,

<http://www.emptywheel.net/2014/05/16/the-automated-query-at-the-telecoms-will-include-correlations>.

مارسي وييلر (28 يونيو 2014). موقع «إيمبتي وييل»، مقال: «العملية المحسنة الجديدة لوكالة الأمن القومي» في ربط سلاسل المكالمات؛ لا تتطلب حدوث اتصالات هاتفية».

Empty Wheel,

<http://www.emptywheel.net/2014/06/28/nsas-new-and-improved-call-chaining-process-now-with-no-calls-required>.

38. يحمل البرنامج اسماً شيفراً هو «كوترافلر» (CO-TRAVELLER). بارتون غيلمان وأشكان سلطاني (4 ديسمبر 2013). صحيفة واشنطن بوست. مقال: «وفق وثائق سنودن، «وكالة الأمن القومي» تتبّع مواقع الخلويات عالمياً».

Washington Post,

http://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowdendocuments-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html.

39. إدارة «وكالة الأمن القومي» (2012). «ملخص عن الأدوات التحليلية في برنامجي «دي أن آر» و«كوترافلر»». https://www.eff.org/files/2013/12/11/20131210-wapo-cotraveler_overview.pdf.

40. جوليان سانشير (11 أكتوبر 2013). «جاست سيكيورتي». مقال: «استعمالات أخرى للقاعدة بيانات الهواتف لدى «وكالة الأمن القومي»: إيجاد بصمات أصحاب الهواتف المحروقة؟»

Just Security,

<http://justsecurity.org/2013/10/11/nsa-call-records-database-fingerprinting-burners>

41. بارتون غيلمان وأشكان سلطاني (4 ديسمبر 2013). صحيفة واشنطن بوست، مقال: «وكالة الأمن القومي» تتعقب الخليويات في العالم كله، وفق وثيقة من سنودن.

Washington Post,

http://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html.

42. تعمل تلك التقنية الأساسية في برنامج «كوترافلر». إذا كان هنالك هاتف يستخدم دوماً الشبكة التي يستعملها هاتفك الرئيس، فالأرجح أنه في جيبك. وزارة العدل الأميركية (13 فبراير 2012). «شكوى جرمية». الولايات المتحدة ضد جوزيه أغويو وآخرون. (رقم القضية محظور).

United States District Court, Northern District of Illinois, Eastern Division,

http://www.justice.gov/usao/iln/pr/chicago/2013/pr0222_01d.pdf.

43. هياواتا براي (24 إبريل 2014). مجلة ديسكوفر. مقال: «كيف ترسم التطبيقات المستندة إلى الموقع الجغرافي مستقبل التّبضع».

Discover,

<http://blogs.discovermagazine.com/crux/2014/04/30/how-location-based-apps-will-shape-the-future-of-shopping>

44. لورين جونسون (9 يونيو 2014). لماذا تعمل مايكروسوفت على نشر الإعلانات المستندة إلى الموقع الجغرافي عند مخازن البيع بالفرق: الاختبارات أعلت شأن حركة المشاة. جريدة بوسطن غلوب.

Boston Globe,

<http://www.bostonglobe.com/business/2013/07/07/your-cellphone-ourselvesvTK1UCqNOE7D4qbAcWPL/story.html>.

45. هياواتا براي (8 يوليو 2013).

Boston Globe,

<http://www.bostonglobe.com/business/2013/07/07/your-cellphone-yourselfeSvTK1UCqNOE7D4qbAcWPL/story.html>.

46. ألي وينستون (17 يونيو 2014). «مركز التقارير الاستقصائية». مقال: «خطط للتوسع في أمدية القارات الضوئية للوحات المركبات، وفق تحذير من محامين».

Center for Investigative Reporting,

<http://cironline.org/reports/plans-expand-scope-licenseplate-readers-alarm-privacy-advocates-6451>.

47. يناقش المقال التالي خطط الداف بي أي في فعل ذلك تحديداً. «مركز معلومات الخصوصية الإلكترونية» (ديسمبر 2013). «الجيل التالي من برامج الداف بي أي» في التعرف: نظام «الأخ الكبير» الهوية؟

Spotlight on Surveillance,

<https://epic.org/privacy/surveillance/spotlight/ngi.html>.

48. برزت مخاوف بشأن استخدام بطاقات «أويستر» عندما ظهرت تلك التقنية في لندن سنة 2003. هيئة «بي بي سي». آرون شيلليون (25 سبتمبر 2003) مقال: «بطاقة ذكية تتعقب مستخدميه».

BBC News,

<http://news.bbc.co.uk/2/hi/technology/3121652.stm>.

49. غريغ ويستون، غلين غرينوود وراين غالاهاار (30 يناير 2014). تلفزيون «سي بي سي نيوز». مقال: «وكالة «سيسك» استخدمت الدواي فاي» في المطار لتتبع مسافرين كنديين، وفق وثائق سنودن.

CBC News,

<http://www.cbc.ca/news/politics/csecused-airport-wi-fi-to-track-canadian-travellers-edward-snowden-documents-1.2517881>.

50. أليساندرو أكويستي، رالف كروس وفريد شتوتزمان (4 أغسطس 2011). مقال: «وجوه» فيسبوك: الخصوصية في زمن الحقيقة المدعومة رقمياً.

Black Hat 2011, Las Vegas, Nevada,

<http://www.heinz.cmu.edu/~acquisti/face-recognition-study-FAQ/acquisti-faces-BLACKHAT-draft.pdf>

51. سكوت إللارت (7 ديسمبر 1999). «نظم ووسائل للمناقلة البيانات بين قواعد البيانات (5999937)». المكتب الأمريكي للعلامات التجارية وبراءات الاختراع.

<http://www.google.com/patents/US5999937>

52. كوتون ديلو (22 فبراير 2013). مقال: «فيسبوك» يتشارك مع برنامج «إيسلون» من شركة «أكزيكوم» في مطابقة قوائم الشراء في المخازن مع بروفائلات مستخدميه.

Advertising Age,

<http://adage.com/article/digital/facebook-partner-acxiom-epsilon-match-storepurchases-user-profiles/239967>.

53. كارولين كوبر وكلي غوردون (2 إبريل 2014). الموقع الشبكي لقناة «الجزيرة». مقال: «هناك من يربح من معلومات عن عاداتك في الشرب وأمراضك المنقولة جنسياً».

Al Jazeera,

<http://america.aljazeera.com/watch/shows/america-tonight/articles/2014/4/2/the-people-makingmoneyoffyourdrinkinghabitsandstds.html>.

54. ماكس فيشر (19 فبراير 2013). صحيفة واشنطن بوست. مقال: «الهاكرز» الصينيون كشفوا أنفسهم بدخولهم إلى حساباتهم الشخصية على «فيسبوك».

Washington Post,

<http://www.washingtonpost.com/blogs/worldviews/wp/2013/02/19/chinese-hackers-outed-themselves-by-logging-into-their-personal-facebook-accounts>

55. بول روبرتس (7 مارس 2012). «الثرثرات على الدويب»، وحوادث السيّارات، وممارسة النسخ واللصق، زرعت بذور مأساة مونزيغر.

Threatpost,

<http://threatpost.com/chats-carcrashes-and-cut-n-paste-sowed-seeds-lulzsecs-demise-030712/76298>.

56. كريس سوفيغان (13 نوفمبر 2012). مقال: «الرقابة ودروس الأمن المستقاة من فضيحة باولا برديويل». «الاتحاد الأمريكي للحريات المدنية».

American Civil Liberties Union,

<https://www.aclu.org/blog/technology-and-liberty-national-security/surveillance-and-security-lessons-petraeus-scandal>.

57. دان أوكس (12 إبريل 2012)، صحيفة سيدني هيرالد مورنينغ. مقال: «حال أعطى فيها «هاكر» جسماً من الأدلة».

Sydney Morning Herald,

<http://www.smh.com.au/technology/technology-news/hacking-cases-body-of-evidence-20120412-1wsbh.html>.

58. رونين برغمان وآخرون (17 يناير 2011) صحيفة دير شبيغل. مقال: «عيناً بعين: تفاصيل عملية الموساد الإسرائيلي في دبي».

Der Spiegel,

<http://www.spiegel.de/international/world/an-eye-for-an-eye-the-anatomy-of-mossad-sdubai-operation-a-739908.html>.

59. بول أوم (13 أغسطس 2009). ورقة بحث: «وعد الخصوصية المكسور: في الاستجابة للفشل الذريع لتقنيات إخفاء الهوية».
UCLA Law Review 57,
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006.
60. ميشيل باربيرو وتوم زيلر جونيور (9 أغسطس 2006). صحيفة نيويورك تايمس. مقال: «الكشف عن هوية صاحب عملية البحث رقم 4417749 على موقع «إيه أو أل»».
New York Times,
<http://www.nytimes.com/2006/08/09/technology/09aol.html>.
61. أرفاند نارايان وفيتالي شماتيكوف (18-20 مايو 2008). ورقة بحث: «كشف الهويات المخفية بطريقة مكنية استناداً إلى قواعد بيانات مبعثرة».
2008 IEEE Symposium on Security and Privacy, Oakland, California,
<http://dl.acm.org/citation.cfm?id=1398064> and
http://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf
62. ولغايات بحثية في منتصف التسعينيات من القرن الماضي، نشرت «لجنة الضمان في مجموعة ماساشوستس» ملفات المستشفيات لموظفي الدولة بعد أن أزلت منها الأسماء والعناوين وأرقام الضمان الاجتماعي. وبرهنت عائلة الكمبيوتر لاتانيا سويني، وكانت حينها طالبة موشكة على التخرج من «معهد ماساشوستس للتقنية»، أنها استطاعت كسر إغفال الهوية في الملفات بربطها بتواريخ الميلاد وأرقام مشاريع البلدية من جهة، وقاعدة بيانات لتسجيل الناخبين. لاتانيا سويني (يونيو 1997)، ورقة بحث: «حيك التكنولوجيا والسياسة معاً لضمان السرية».
Journal of Law, Medicine and Ethics 25,
<http://onlinelibrary.wiley.com/doi/10.1111/j.1748-720X.1997.tb01885.x/abstract>.
63. لاتانيا سويني (2000). بحث: «المعلومات الديموغرافية البسيطة تكفي أحياناً للتعرف إلى هوية متفردة».
جامعة «كارنيغي- ميلون». ورقة بحث رقم 3 بشأن بيانات الخصوصية.
Carnegie Mellon University, Data Privacy Working Paper 3,
<http://dataprivacylab.org/projects/identifiability/paper1.pdf>.
64. فيليب غول (30 أكتوبر 2006). ورقة بحث: «إعادة البحث في فريدة المعلومات في البيانات الديموغرافية عن سكان الولايات المتحدة».
population,» 5th ACM
Workshop on Privacy in the Electronic Society (WPES'06), Alexandria, Virginia,
<http://crypto.stanford.edu/~pgolle/papers/census.pdf>
65. ميليسا غايمرك وفريقها (18 يناير 2013). مجلة ساينس، ورقة بحث: «التعرف إلى الحمض النووي للأفراد استناداً إلى استدلال من اسم العائلة».
Science 339,
<http://www.sciencemag.org/content/339/6117/321.abstract>.
- جون بوحتون وآخرون. مجلة ساينس، ورقة بحث: «قواعد البيانات عن شجرة العائلة تكشف أسماء المتبرعين المغلي الهوية للحمض النووي».
Science 339,
<http://www.sciencemag.org/content/339/6117/262>.
66. آدم تانر (11 أكتوبر 2013). مجلة فوربس. مقال: «الغوص في البيانات يكشف هويات المشاركين في البحوث الجنسية».
Forbes,
<http://www.forbes.com/sites/adamtanner/2013/10/11/decoding-the-secrets-of-sex-data>
67. أرفاند نارايان وفيتالي شماتيكوف (يونيو 2010). بحث: «أوهام وخرافات المعلومات المعروفة بالهوية».
Communications of the ACM 53,
<http://dl.acm.org/citation.cfm?id=1743558>.

68. رايمان غالاهار (25 أغسطس 2014). موقع «إنترسبت». مقال: «مركز الرقابة: كيف صنعت «وكالة الأمن القومي» محرك بحثها السري المشابه لـ«غوغل»».

Intercept,

<https://firstlook.org/theintercept/2014/08/25/icreach-nsa-cia-secret-google-crisscross-proton>.

69. إيف ألكسندر دي مونتجوي وآخرون. (4 فبراير 2013). موقع «نايتشر». مقال: «متفرد وسط الحشد: حدود الخصوصية في الحراك الإنساني».

Scientific Reports 3, Article 1376,

<http://www.nature.com/srep/2013/130325/srep01376/full/srep01376.html>.

70. لا أقصد القول باستحالة تجهيل هوية مجموعة ما من البيانات، لكنني أقول إن ذلك صعب جداً ومن السهل الوقوع في الخطأ بشأنه. إذ يعتقد كثيرون بأن استبدال بيانات حساسة بأرقام عشوائية، يكفي لحمايتها، لكن ذلك خطأ. ففي أغلب الأحيان، لا ينفع ذلك الإجراء كلياً.

71. من المستطاع أن تضرب مثلاً بقوانين «وزارة الأمن الوطني». ماري إلين غالاهان (مارس 2012). كتاب عن تأمين المعلومات المعروفة بالخصوصية. وزارة الأمن الوطني في الولايات المتحدة.

http://www.dhs.gov/sites/default/files/publications/privacy/Guidance/handbookforsafeguardingsensitivePII_march_2012_webversion.pdf.

الفصل 4: تجارة الرقابة

1. كايبي هاويز (16 أكتوبر 2013). موقع «غازيل». مقال: «استعمل تطبيق الدفلاش، للخداع أو التعامل».

Gazelle,

<https://www.gazelle.com/thehorn/2013/10/16/use-yourflashlight-app-for-trick-or-treating>

2. سيسيليا غانغ (5 ديسمبر 2013). صحيفة واشنطن بوست. مقال: «تطبيق للدفلاش» يبيقي في الظلام أنه يتشارك في «البيانات المكانية».

Washington Post,

http://www.washingtonpost.com/business/technology/flashlight-app-kept-users-in-the-dark-about-sharing-location-data-ftc/2013/12/05/1be26fa6-5dc7-11e3-be07-006c776266ed_story.html.

3. جيسون هونغ (30 نوفمبر 2012). مقال: «تحليل عن تطبيق «برايتست فلاش لايت فري» لهواتف الدأندرويد».

Jason Hong's Confabulations,

<http://confabulator.blogspot.com/2012/11/analysis-of-brightest-flashlight-free.html>

4. «اللجنة الفيدرالية للتجارة» (5 ديسمبر 2013). ورقة: «مطور تطبيق «فلاش لايت» للدأندرويد» يسوّي اتهامات «لجنة التجارة الفيدرالية» بأنه خدع المستهلكين: «برايتست فلاش» تشارك بيانات مكان المستخدم وهوية هاتفه، من دون تعريف المستهلكين بذلك».

<http://www.ftc.gov/news-events/press-releases/2013/12/android-flashlight-app-developer-settles-ftc-charges-it-deceived>.

5. أحياناً، تفرض الرقابة بالإكراه. وكى أحصل على ضمان لساعة ما، غالباً ما يفرض علي إعطاء معلومات إلى الشركة التي صنعت تلك الساعة.

6. خلال أيام من البحث على «غوغل» عن مكان لقضاء إجازة، بدأت في تلقي إعلانات من «ترافيلوستي» عن ذلك المكان. ولا أملك حساباً في موقع «ترافيلوستي».

7. بيتر إكرسلي (21 سبتمبر 2009). «مؤسسة الحدود الإلكترونية». مقال: «كيف تتعرّف الشركات التي تتبّعك على الويب»، معظم ما تفعله (وكيف تساعدك شركات الدسوشال ميديا في ذلك).
Electronic Frontier Foundation,
<https://www.eff.org/deeplinks/2009/09/online-trackers-and-social-networks>.
8. صاموئيل غيبس (28 أكتوبر 2013). صحيفة الغارديان. مقال: «أداة «لايت بيم» من محرّك البحث «فايرفوكس» تظهر لك من يلاحقك على الإنترنت».
Guardian,
<http://www.theguardian.com/technology/2013/oct/28/mozilla-lightbeam-tracking-privacy-cookies>
9. 241 أليكس مادريغال (29 فبراير 2012). مجلة أتلانتك. مقال: «أنا ملاحق. كيف عمد «غوغل» - و 104 شركات أخرى- إلى ملاحظتي على الإنترنت».
<http://www.theatlantic.com/technology/archive/2012/02/im-being-followedhow-google-151-and-104-other-companies-151-are-tracking-me-on-the-web/253758>.
10. جوليا أنغوين (30 يوليو 2010). صحيفة وول ستريت جورنال. «منجم الذهب الجديد على الإنترنت: أسرارك».
<http://online.wsj.com/news/articles/SB10001424052748703940904575395073512989404>
11. أندرو كانينغهام (5 يوليو 2013). موقع «أرس تكنيكا». مقال: «شركة سامسونغ وجاي- زي يعطون درساً متقدماً في ما لا يجب فعله في التطبيقات الرقمية».
Ars Technica,
<http://arstechnica.com/gadgets/2013/07/samsung-and-jay-z-give-the-internet-amateurs-class-in-how-not-to-make-an-app>.
12. فرانسيس شانغ، فومينغ شيه وداينال فايتزنر. (4-8 نوفمبر 2013). ورشة عمل عن الخصوصية في المجتمع الإلكتروني، برلين، ألمانيا. ورقة بحث: «لا مفاجآت: قياس مدى تدخلية تطبيقات الخواري بقياس الانحرافات عن السياق».
12th ACM Workshop on Privacy in the Electronic Society (WPES'13), Berlin, Germany,
<http://dl.acm.org/citation.cfm?id=2517864>
13. دوغلاس راشكوف (6 يوليو 2012). شبكة «سي آن أن». «هل يتجسّس مقدم خدمة الإنترنت عليك؟»
CNN,
<http://www.cnn.com/2012/07/06/opinion/rushkoff-online-monitoring>.
ديفيد كرافتس (5 فبراير 2013). مجلة وايرد. «أصبح مقدّمو خدمة الإنترنت يبحثون الآن عن التبعيات على حقوق الملكية الفكرية».
14. كايي جونستون (3 ديسمبر 2012). «كيف تصبح مُراقباً من جهاز التلفزيون؟ جرّب وضع كاميرا على جهاز الربط مع الإنترنت».
Ars Technica,
<http://arstechnica.com/tech-policy/2012/12/how-to-get-targeted-ads-on-your-tv-a-camera-in-your-settop-box>.
كريستوفر زارا (26 يوليو 2013). «هل يتجسّس جهاز الكابل التلفزيوني عليك؟ إنّ نشاط الخصوصية يخشون أن مايكروسوفت وقاريزون تفعله».
International Business Times,
<http://www.ibtimes.com/your-cable-box-spying-you-behavior-detecting-devices-verizon-microsoft-others-worry-privacy-1361587>

15. إنه أمر مثير أننا نستخدم أفكاراً آتية من عالم الخيال في وصف مجريات الرقابة والخصوصية، كوصفها بالأيروبية أو الكافكاوية أو بما وصفه تولكين في رواية عين على سورون. بروس شناير (18 إبريل 2014)، «المجاز في الرقابة». كتاب شناير: عن الأمن.

https://www.schneier.com/blog/archives/2014/04/metaphors_of_su.html.

16. بيتر إكرسلي (يوليو 2010). ورقة بحث: «ما مدى فريدة متصفحك للإنترنت؟» *Proceedings of the 10th International Conference on Privacy Enhancing Technologies*, <https://panopticklick.eff.org/browser-uniqueness.pdf>.

كيتون ماوري وهوفاف شاتشام (24 مايو 2012). «مكتمل بالبيكسل: بصمات في نسيج «أنش تي أم آل 5». Web 2.0 Security and Privacy, San Francisco, California, <http://cseweb.ucsd.edu/~hovav/papers/ms12.html>

جوليا أنغوين (21 يوليو 2014). مقال: «تعرف إلى أداة الملاحقة على «الويب» التي يستحيل صدّها نظرياً». موقع «بروبابليكا».

Pro Publica,

<http://www.propublica.org/article/meet-the-online-tracking-device-that-is-virtually-impossible-to-block>.

غونيس آكار وآخرون (10 أغسطس 2014). ورقة بحث: «الإنترنت لا تنسى أبداً: انفلات ميكانيزمات الملاحقة». ACM Conference on Computer and Communications Security (CCS 2014), Scottsdale, Arizona,

<https://securehomes.esat.kuleuven.be/~gacar/persistent/index.html>.

17. «غوغل» (5 يوليو 2014). رد على تدوين: إزالة القيود على مستخدمي «غوغل+». <https://plus.google.com/+googleplus/posts/V5XkYQYYJqy>.

18. يعيد «فيسبوك» النظر في سياسته تلك، بعد مواجهات مع مستخدمين تضرّروا منها. Facebook (2014), «What names are allowed on Facebook?», <https://www.facebook.com/help/112146705538576>.

رييد ألبرغوتي (2 أكتوبر 2014). صحيفة وول ستريت جورنال. مقال: «فيسبوك يغيّر سياسة الاسم الحقيقي، بعد زوبعة احتجاج من متبنّرين».

Wall Street Journal,

<http://online.wsj.com/news/articles/SB10000872396390444165804578008740578200224>.

19. تغيّر موقف الناس حيال دفع المال، إلى حدّ ما. إذ يدفع كثيرون منا أموالاً قليلة، أو حتى كثيرة مقسّطة لزمان طويل، للحصول على تطبيقات للخلوي، لكن منحى الرقابة في الأعمال على الإنترنت لم يتبدّل. وحتى التطبيقات التي تدفع مالاً لقاء الحصول عليها، تتجسّس عليك.

20. سكوت برادونر (3 أغسطس 2010). «نتورك ورلد». مقال: «ثمن الإنترنت المجاني: قطعة من روحك».

Network World,

<http://www.networkworld.com/columnists/2010/080310bradner.html>

21. كورت أويساهل (28 إبريل 2010)، «مؤسّسة الحدود الإلكترونية». «مراجعة: تآكل سياسة «فيسبوك» للخصوصية».

Electronic Frontier Foundation,

<https://www.eff.org/deeplinks/2010/04/facebook-timeline>

22. هناك رسم توضيحي تفاعلي بنوعية ممتازة عن ذلك الموضوع: مات ماكينون (15 مايو 2010). مدوّنة إلكترونية. «تطوّر الخصوصية على «فيسبوك»».

<http://mattmckeeon.com/facebook-privacy>.

23. شبكة «سي تي في نيوز» عن «وكالة أسوشيتد برس». «مراجعة زمنية: نظرة إلى التطورات المتصلة بسياسة «غوغل» بشأن الاهتمامات المتعلقة بالخصوصية».

CTV News,

<http://www.ctvnews.ca/sci-tech/timeline-a-look-at-developments-linked-to-google-privacyconcerns-1.1220927>.

24. ريتش موغول (25 يونيو 2014). مجلة ماك وورلد. مقال: «لماذا تهتم «آبل» فعلياً بخصوصيتك؟»

Macworld,

<http://www.macworld.com/article/2366921/why-apple-really-cares-about-your-privacy.html>

25. تشارلز آرثر (18 سبتمبر 2014). صحيفة الغارديان. مقال: «تيم كوك، رئيس «آبل»، يهاجم «غوغل» و«فيسبوك» بسبب ثغرات في الخصوصية».

Guardian,

<http://www.theguardian.com/technology/2014/sep/18/apple-tim-cook-google-facebook-privacy-surveillance>.

26. جاي غريني (18 مارس 2014). «شركة «أمازون» تدخل بيسر تجارة جانبية قيمتها بليون دولار: الإعلانات عن التخفيضات».

Union Bulletin,

<http://union-bulletin.com/news/2014/mar/18/amazon-easing-1b-sideline-business-ad-sales>

ناديا توما ولورا سمبسون (23 يناير 2014)، مجلة أدفرتايزنغ آيج، «لماذا لا يخاف الناس من تخزين البيانات في «أمازون»، بينما يخافونها في «فيسبوك»؟

Advertising Age,

<http://adage.com/article/guest-columnists/americans-scared-amazon-s-data-store/290953>

27. أمي حرمون (24 أغسطس 2001). صحيفة نيويورك تايمس، مقال: «مع وضع البيانات العامة على الإنترنت، يعتقد البعض أنها باتت عامة بصورة فائضة».

New York Times,

<http://www.nytimes.com/2001/08/24/nyregion/as-public-records-go-online-some-say-they-re-too-public.html>

مارك أكرمان (26 أغسطس 2013). مقال: «بيع البيانات العامة إلى المسوقين يدر أموالاً كثيرة على الحكومات».

CBS Denver,

<http://denver.cbslocal.com/2013/08/26/salesof-public-data-to-marketers-can-mean-big-for-governments>

28. ثمة مقال جيد عن «أكزيوم»، ناتاشا سنغر، (16 يونيو 2012)، صحيفة نيويورك تايمس، «رسم الخرائط الجينية للزيائن وبيعها».

New York Times,

<http://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html>.

29. يقدر «المنتدى العالمي للخصوصية» أن هناك قرابة 4 آلاف سمسار للمعلومات. بام ديكسون (18 ديسمبر 2013). «شهادة بام ديكسون، المدير التنفيذي لـ«المنتدى العالمي للخصوصية» أمام «لجنة التجارة والعلوم والمواصلات»، في مجلس الشيوخ الأمريكي: ما هي المعلومات التي يملكها سمسار البيانات عن المستهلكين، وكيف يستخدمونها؟

World Privacy Forum,

<http://www.worldprivacyforum.org/2013/12/testimony-what-information-do-data-brokers-have-on-consumers>

30. كريغ تيمبرغ (27 مايو 2014). صحيفة واشنطن بوست. مقال: «سماسرة البيانات يستعملون «بلايين» النقاط لرسم بروفائلات عن الأميركيين».

Washington Post,

http://www.washingtonpost.com/business/technology/brokers-use-billions-of-data-points-to-profile-americans/2014/05/27/b4207b96-e5b2-11e3-a86b-362fd5443d19_story.html.

31. أجرت صحيفة وول ستريت جورنال سلسلة تحقيقات عن الكميات الضخمة من بيانات الرقابة التي تجمعها شركات مختلفة. نشرت تلك التحقيقات تحت اسم مرجعي «ما الذي يعرفونه؟»، وتتوافر على موقع الصحيفة. *Wall Street Journal*, «What They Know» series index,

<http://online.wsj.com/public/page/whatthey-know-digital-privacy.html>.

32. «لجنة التجارة والعلوم والمواصلات»، في مجلس الشيوخ الأمريكي، «مكتب الإشراف والمراقبة». طاقم موظفي الأغلبية (18 ديسمبر 2013). «مراجعة بصدد صناعة سماسرة المعلومات: جمع بيانات المستهلكين واستخدامها وبيعها لأغراض تسويقية». تقرير الطاقم المقدم إلى رئيس الأغلبية روكفلر.

http://consumercal.org/wpcontent/uploads/2013/12/senate_2013_data_broker_report.pdf

33. لويس بيكيت (13 سبتمبر 2013). موقع «بروبابليكا»، مقال: «كل ما نعرفه عما يعرفه سماسرة البيانات عنك».

Pro Publica,

<https://www.propublica.org/article/everything-we-know-about-what-data-brokers-know-about-you>

34. ناتاشا سنغر (5 سبتمبر 2013). صحيفة نيويورك تايمس. مقال: «شركة «أكزيوم» تتيح للمستهلكين رؤية البيانات التي تجمعها».

New York Times,

<http://www.nytimes.com/2013/09/05/technology/axiom-lets-consumers-see-data-it-collects.html>

35. 267 تشارلز دوهيغ (20 مايو 2007). صحيفة نيويورك تايمس. مقال: «مخادعة المسنين، مع دعم من الشركات».

New York Times,

<http://www.nytimes.com/2007/05/20/business/20tele.html>.

36. «لجنة التجارة والعلوم والمواصلات»، في مجلس الشيوخ الأمريكي، «مكتب الإشراف والمراقبة». طاقم موظفي الأغلبية (18 ديسمبر 2013). «مراجعة بصدد صناعة سماسرة المعلومات: جمع بيانات المستهلكين واستخدامها وبيعها لأغراض تسويقية». تقرير الطاقم المقدم إلى رئيس الأغلبية روكفلر.

http://consumercal.org/wp-content/uploads/2013/12/senate_2013_data_broker_report.pdf

37. جوزيف تودو (7 فبراير 2012)، مجلة أتلانتيك، مقال: «دليل إرشادي إلى صناعة الإعلام الرقمي التي تتجسس على كل نقرة تجريها».

Atlantic,

<http://www.theatlantic.com/technology/archive/2012/02/a-guide-to-the-digital-advertisingindustry-thats-watching-your-every-click/252667>.

38. ليس معروفاً من قال تلك العبارة أولاً. جوناثان زيترتين (21 مارس 2012)، «المدونات الإلكترونية لجامعة هارفرد». «قول سار: «إذا كان شيء ما مجانياً، فأنت لست المستهلك بل المنتج».

The Future of the Internet and How to Stop It,

<http://blogs.law.harvard.edu/futureoftheinternet/2012/03/21/meme-patrol-when-something-online-is-free-youre-not-the-customer-youre-the-product>

39. نلسون وايت (7 نوفمبر 2013)، صحيفة فانكوفر صن، مقال: «النائب السابق للرئيس الأمريكي آل غور، يتوقع أن يكسب المشرعون معركة الرقابة».

Vancouver Sun,

<http://www.vancouversun.com/news/Former+vicepresident+Gore+predicts+lawmakers+will+rein/9129866/story.html>.

40. لورانس غرين (5 يوليو 2010)، صحيفة التلغراف، مقال: «لماذا يعطيك الابتكار نجاحاً أكبر مما يفعله المال».

Telegraph,

<http://www.telegraph.co.uk/finance/businessclub/7872084/Why-creativity-will-buy-you-more-success-than-money.html>.

41. على الأقل، ذلك ما تقوله النظريات. هناك من يحتاج بأن ذلك ليس بالكفاءة المرجوة. دوجلان راشكوف (2013). كتاب صدمة الحاضر: عندما يحدث كل شيء الآن.

Present Shock: When Everything Happens Now, Current,

<http://www.rushkoff.com/present-shock>.

42. «ريل غرين سيستمز» (2014). «المساعدة في القياس: تطبيق شبكي يجمع الصور الجوية مع أدوات القياس».

https://www.realgreen.com/measurement_assistant.html.

43. ناثان أبز (أكتوبر 2012). «تأثير البيانات الضخمة» على مآل الحملات السياسية: الإعلان السياسي الموجه إلى مجموعات ميكروية في انتخابات الرئاسة للعام 2012.

Interactive Advertising Bureau,

http://www.iab.net/media/file/Innovations_In_Web_Marketing_and_Advertising_delivery.pdf

44. مايكل شير (7 نوفمبر 2012)، مجلة تايم، مقال: «العالم الداخلي للتهيبي البيانات الذين ساعدوا في فوز أوباما».

Time,

<http://swampland.time.com/2012/11/07/inside-the-secret-world-of-quants-and-data-crunchers-who-helped-obama-win>.

ساشا آيزنبرغ (19 ديسمبر 2012). موقع «إم آي تي تكنولوجي ريفيو»، مقال: «كيف استعملت حملة الرئيس أوباما البيانات الضخمة في تعبئة الناخب الفرد».

MIT Technology Review,

<http://www.technologyreview.com/featuredstory/509026/how-obamas-team-used-big-data-to-rally-voters>

45. إد بلنكينغتون وأماندا ميشيل (17 فبراير 2012)، صحيفة الغارديان، «أوباما و«فيسبوك» وقوة الصداقة: البيانات في حملة 2012 الانتخابية».

Guardian,

<http://www.theguardian.com/world/2012/feb/17/obama-digital-data-machinefacebook-election>

تاتزينا فيفا (20 فبراير 2012)، صحيفة نيويورك تايمز، «بيانات شبكية ساعدت في توجيه الإعلانات في حملة 2012 الانتخابية».

New York Times,

<http://www.nytimes.com/2012/02/21/us/politics/campaigns-use-microtargeting-to-attract-supporters.html>

46. حاضراً، يسمح لك كثيرون من سمسرة المعلومات بتصحيح الأخطاء في بياناتهم. ويساهم كل تصحيح تجريه في تحسين نوعية البيانات التي يبيعونها لآخرين. إن تصحيحك تساعدهم، لكنهم يقدمونها كأنها نوع من الحق الذي اكتسبته الآن.

47. في العام 2014، أرسلت شركة «شاترفلاي» رسائل إلى الناس تهنئهم بالمواليد الجدد، وارتكبت بعض الأخطاء. وتكفلت تلك الأخطاء بوصول الأمر إلى الصحافة. كشمير هيل (14 مايو 2014)، مجلة فوربس، مقال: «شركة «شاترفلاي» ترسل تهنئة بدالقام الجديد» لأشخاص ليس لديهم أطفال».

Forbes,

<http://www.forbes.com/sites/kashmirhill/2014/05/14/shutterfly-congratulates-a-bunch-of-people-without-babies-on-their-new-arrivals>.

48. تتوافر دلائل ظرفية كثيرة عن كيفية إفساد الإعلانات الموجهة خطأ للأمور، لكن معظمها يأتي من كوننا نلاحظ الأخطاء أكثر من التنبيه إلى المسار الرئيس للأمر.

49. جلال محمود، جيفري نيكولاس وكليمانس دروس (7 مارس 2014). «تحديد منازل مستخدم «تويتر»». *arXiv:1403.2345 [cs.SI]*, <http://arxiv.org/abs/1403.2345>

50. هناك مقال يناقش كفاءة الإعلان بواسطة الإنترنت. دريك طومسون (13 يونيو 2014). مجلة *أتلانتيك*. مقال: «سؤال خطير: هل هناك أي فعالية على الإطلاق للإعلان بواسطة الإنترنت؟»

Atlantic,

<http://www.theatlantic.com/business/archive/2014/06/a-dangerous-question-does-internet-advertising-work-at-all/372704>.

51. في 2014، أرسلت شركة «أوفيس ماكس» بريدًا ترويجيًا موجهًا إلى «مايك سايي» / طفلة قضت أثناء حادث سيارة / أو في تجارة جارية». نجم ذلك البريد عن خطأ في قاعدة البيانات، لكنه يبين مدى دقة المعلومات التي يجمعها سماسرة البيانات. أمي ميرك (23 يناير 2014). صحيفة *نيويورك*. مقال: «موت في قاعدة البيانات».

New Yorker,

<http://www.newyorker.com/online/blogs/currency/2014/01/ashley-seay-officemax-carcrash-death-in-the-database.html>

52. بليز أور وآخرون (2 إبريل 2012). جامعة «كارينغي ميلون». «ذكى، مفيد، مخيف ومرعب: انطباعات عن الإعلان الموجه وفق السلوك».

CyLab, Carnegie Mellon University, Pittsburgh, Pennsylvania,

https://www.cylab.cmu.edu/research/techreports/2012/tr_cylab12007.html

53. فارهاد مانجو (23 أغسطس 2012)، موقع «سلايت». مقال: «الوادي غير الحاذق في إعلانات الإنترنت».

Slate,

http://www.slate.com/articles/technology/technology/2012/08/the_uncanny_valley_of_internet_advertising_why_do_creepy_targeted_ads_follow_me_everywhere_i_go_on_the_web.html.

سارة وإطلسون (16 يونيو 2014). مجلة *أتلانتيك*. «بيانات الشبيه الشبهي والوادي غير الحاذق» للشخصية.

Atlantic,

<http://www.theatlantic.com/technology/archive/2014/06/data-doppelgangers-and-the-uncanny-valley-of-personalization/372780>.

54. مايك مازنيك (11 مارس 2008). مجلة *تيك ديرت*. مقال: «أين يرتسم الفاصل بين الإعلان المشخص وإثارة رغبة الناس؟»

Tech Dirt,

<http://www.techdirt.com/articles/20080311/121305499.shtml>

55. بليز أور وآخرون (2 إبريل 2012). جامعة «كارينغي ميلون». «ذكى، مفيد، مخيف ومرعب: انطباعات عن الإعلان الموجه وفق السلوك».

CyLab, Carnegie Mellon University, Pittsburgh, Pennsylvania,

https://www.cylab.cmu.edu/research/techreports/2012/tr_cylab12007.html

56. إيفان سلينغر (22 أغسطس 2012). موقع «سلايت». مقال: «في أننا نحب أن ندعو التكنولوجيا الجديدة بأنها «مرعبة»».

Slate,

http://www.slate.com/articles/technology/future_tense/2012/08/facial_recognition_software_targeted_advertising_we_love_to_call_new_technologies_creepy.html

أومير تيني وجواز بولونتسكي (16 سبتمبر 2013). جامعة «يال»، مجلة التكنولوجيا والقانون. مقال: «نظرية الربيب: التكنولوجيا والخصوصية وتغير الأعراف الاجتماعية».

Yale Journal of Law & Technology,

<http://yjolt.org/theory-creepy-technology-privacyand-shifting-social-norms>.

57. سارة م. واتسون (16 سبتمبر 2014). قناة «الجزيرة» وموقعها الإلكتروني. مقال: «أسأل جهاز فك تشفير قنوات التلفزيون: التريص بالضربات».

Al Jazeera,

<http://america.aljazeera.com/articles/2014/9/16/the-decoder-stalkedbysocks.html>

58. مايك أيزاك (2 نوفمبر 2011). مجلة وايرد. مقال: «سياسة «غوغل» الجديدة في «الشفافية» تهدف إلى خفض الشعور بالارتياح».

Wired,

<http://www.wired.com/2011/11/google-ad-transparency-target>.

تود إيزيك (27 فبراير 2012)، مجلة فوربس، مقال: «ربما توصلك البيانات الضخمة إلى الارتياح، لكن الشفافية تفيد في درته».

Forbes,

<http://www.forbes.com/sites/toddessig/2012/02/27/big-data-got-you-creeped-out-transparency-can-help>

59. تشارلز دوهيغ (19 فبراير 2012). صحيفة نيويورك تايمس. مقال: «كيف تعرف الشركات أسرارك؟»

New York Times,

<http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html>

60. كشمير هيل (21 أغسطس 2013)، مجلة فوربس، مقال: «صعود ظاهرة استعمال برامج صدّ الإعلانات».

Forbes,

<http://www.forbes.com/sites/kashmirhill/2013/08/21/use-of-ad-blocking-is-on-the-rise>

61. فكتور ليكرسون (7 مارس 2014). مجلة تايم. مقال: «قيمة الإعلان على «تويتر» في تدنّ مطرد».

Time,

<http://time.com/16032/twitter-ad-prices-decline>

برايان ووماك (16 إبريل 2014). مقال: «عائدات «غوغل» أقل من التوقعات، وسقوط مردود الإعلانات».

Bloomberg Business Week,

<http://www.businessweek.com/news/2014-04-16/google-revenue-fallsshort-of-estimates-as-ad-prices-decline-1>.

62. إميلي ستيل (13 يونيو 2013). صحيفة فايننشال تايمس. مقال: «الشركات تهرع صوب بيانات المستهلك».

Financial Times,

<http://link.ft.com/r/S4XZQZ8K8I2/9ZND5E/972MV7/VTD3N8/SN/h>

كين فيغريدو (19 يونيو 2013). مقال: «أسعار بيانات المستهلك وقيمتها».

More with Mobile,

<http://www.more-with-mobile.com/2013/06/prices-and-value-ofconsumer-data.html>

63. تريستان لويس (13 سبتمبر 2013). مجلة فوربس. مقال: «كم يساوي المستهلك الفرد؟»

<http://www.forbes.com/sites/tristanlouis/2013/08/31/how-much-is-a-user-worth>

64. تيم هوانغ وأدي كامدار (9 أكتوبر 2013). مقال: «نظرية الذروة في الإعلانات ومستقبل الإنترنت».

Peakads.org,

http://peakads.org/images/Peak_Ads.pdf.

تيم هوانغ (19 مارس 2014). مقال: «مؤسسة الذروة في الإعلانات».

Knight News Challenge,

<https://www.newschallenge.org/challenge/2014/feedbackreview/the-peak-advertising-institute>

65. دوك سيرلز (23 مارس 2009). مدونة إلكترونية على «بلوغز» جامعة هارفرد. مقال: «ما بعد انفجار فقاعة الإعلانات».
Doc Searls Weblog,
<http://blogs.law.harvard.edu/doc/2009/03/23/after-the-advertising-bubble-bursts>
66. موشيه يودكوفسكي (2005). «كرة الثلج والانهار الثلجي: كيف يؤدي تفكيك الأشياء إلى ثورات». دار نشر «بيريت- كويهلر».
<http://www.pebbleandavalanche.com>
67. مارك غراهام (2008). كتاب الجغرافيات المترابطة للتنمية: الإنترنت ونظريات النمو الاقتصادي. «جيوغرافي كومباس 3/2».
<http://www.geospace.co.uk/files/compass.pdf>
68. 300 مايك مازنيك (19 يونيو 2013). موقع «تيك ديرت». مقال: «المقولات الجديدة في هوليوود: حراس البوابات مذهلون».
Tech Dirt,
<https://www.techdirt.com/articles/20130613/18243923466/hollywoods-new-talking-point-gatekeepersare-awesome.shtml>
69. أليانا م. شيركو وروبرت ج. كوفمان (1998) «مركز البحوث عن نظم إدارة المعلومات». ورقة بحث: «تحليل تحولات السوق في ظل اختفاء الوسطاء بتأثير الإنترنت: دراسة حال عن مقدمي خدمات حجز الطيران بواسطة الإنترنت».
Management Information Systems Research Center,
<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.196.4820&rep=rep1&type=pdf>
70. تيم ويليامز (3 يونيو 2013). شبكة «لينكدن». مقال: «اختفاء الوسطاء في أعمال وكالة الإعلان».
LinkedIn,
<http://www.linkedin.com/today/post/article/20130603205503-2042198-the-disintermediation-of-the-agency-business>
71. كتاب العصر الرقمي الجديد: إعادة رسم مستقبل الشعوب والأمم والأعمال. دار كنوف.
<http://www.newdigitalage.com>
72. كارل شابيرو وهال فاريان (1998). كتاب قواعد المعلوماتية: دليل إرشادي إلى اقتصاد الشبكة. دار «هارفرد بيزنس ريفيو برس».
Harvard Business Review Press,
<http://www.inforules.com>
73. موقع «كوم سكور» (21 يونيو 2014). دراسة «كوم سكور» تنشر تقييمات شهر يونيو 2014 لسوق عمليات البحث».
<https://www.comscore.com/Insights/Market-Rankings/comScore-Releases-June-2014-US-Search-Engine-Rankings>
74. مايف دوغان وآرون سميث (30 ديسمبر 2013). «مشروع بيو لبحوث الإنترنت». ورقة: «تحديث معلومات عن «الدوسال ميديا»».
Pew Research Internet Project,
<http://www.pewinternet.org/2013/12/30/social-media-update-2013>
75. تروي (12 مايو 2013). «مقتطفات من الكتاب الأمريكي للمراجعة السنوية عن ميول المستهلك».
AALB.com's Discussion Forum,
<http://aalbc.com/tc/index.php/topic/2051-highlights-from-the-us-book-consumer-annual-review>

76. تريفيس تيم (24 يوليو 2014)، مجلة فوربس، مقال: «نمو عائدات كومكاست» بـ15% بفضل نمو قوي للبرودباند».
- Forbes*,
<http://www.forbes.com/sites/greatspeculations/2014/07/24/comcast-earnings-grow-15-on-good-broadband-growth>
77. ماثيو فوربدال (2 فبراير 2001)، شبكة «إيه بي سي نيوز»، مقال: «موقع «إي باي» يخفي عناوين البريد الإلكتروني».
- ABC News*,
<http://abcnews.go.com/Technology/story?id=98958>
78. موقع «إي باي» (1 أكتوبر 2011)، «عنوان البريد الإلكتروني وبعض وصلات الإنترنت، لم يعد مسموحاً بهم في القوائم».
- <http://pages.ebay.com/sellerinformation/news/links2011.html>
79. موقع «إي باي» (2 أكتوبر 2012)، «إلى الباعة: عناوين البريد الإلكتروني وبعض وصلات الإنترنت لم يعد مسموحاً بها في التراسل بين مستخدم وآخر».
- <http://announcements.ebay.com/2012/10/sellers-e-mail-addresses-and-someurls-no-longer-allowed-in-member-to-member-messages>
80. ستيفن ليفي (22 إبريل 2014)، مجلة وايرد، «جولة في العلم الذي يوصل تدويناتك المذعورة - الذكية في «فيسبوك» و«تويتر»».
- Wired*,
<http://www.wired.com/2014/04/perfect-facebook-feed>
81. نايت أندرسون (24 يوليو 2008)، مقال: «0.6% لخيار الخروج: «نيبو آد» يخبئ وصلة إلكترونية ضمن 5000 كلمة عن سياسة الخصوصية».
- Ars Technica*,
<http://arstechnica.com/uncategorized/2008/07/06-opt-out-nebuad-hides-link-in-5000-word-privacy-policy>
82. بروس شنابر (26 نوفمبر 2012)، مجلة وايرد، مقال: «في الأمن، عدنا إلى الإقطاع».
- Wired*,
<http://www.wired.com/2012/11/feudal-security>
83. راشيل كينغ (15 أكتوبر 2012)، شبكة «زد نت»، مقال: «تقارير تؤكد أن الجمهور يحب فعلياً بالتأكد التخزين في سحُب المعلومات».
- ZDNet*,
<http://www.zdnet.com/consumers-actually-really-like-cloud-storage-report-says-7000005784>
84. هناك مدخل جيد لشرح «حوسبة السحاب»: ميتشل آرمرست وآخرون (10 فبراير 2009)، تقرير تقني من «جامعة كاليفورنيا - بيركلي»: «فوق السحب: وجهة نظر بيركلي في حوسبة السحاب».
- Technical Report No. UCB/EECS-2009-28, Electrical Engineering and Computer Sciences, University of California at Berkeley,
<http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf>
85. بمبادرة ذاتية منهما، سلّمت شركتا «غوغل» و«مايكروسوفت» أشخاصاً مشتبهاً فيهم بخصوص جنس الطفولة الإباحي إلى الداف بي أي».
- روبرت ماكفرسون (4 أغسطس 2014)، موقع «ياهو نيوز»، مقال: «محرك «غوغل» يدافع عن مبادرته بصدد جنس الطفولة الإباحي».
- Yahoo! News*,
<http://news.yahoo.com/google-defends-child-porn-tip-offs-police-025343404.html>
- ليو كيليون (6 أغسطس 2014)، هيئة «بي بي سي»، مقال: «أدلة من مايكروسوفت أدت إلى اعتقالات بصدد جنس الطفولة الإباحي في بنسلفانيا».

BBC News,

<http://www.bbc.com/news/technology-28682686>.

86. جوناثان زيتترين (2009)، فصل: «معدات مربوطة، وبرامج هي خدمات؛ وتدعيم متكامل»، في كتاب مستقبل الإنترنت وكيف نوقفه، «مطبعة جامعة يال».

Yale University Press,

http://dash.harvard.edu/bitstream/handle/1/4455262/Zittrain_Future%20of%20the%20Internet.pdf

87. ميغ ألبوس (5 سبتمبر 2013). مقال: «كي لا ترفضك «آبل»!

PBS Producer Exchange,

<https://projects.pbs.org/confluence/pages/viewpage.action?pageId=34046325>.

88. براد ستون (18 يوليو 2009). صحيفة نيويورك تايمس. مقال: «أمازون تزيل كتب أورويل من «كيندل».

New York Times,

<http://www.nytimes.com/2009/07/18/technology/companies/18amazon.html>

89. سام غرويارت (14 نوفمبر 2013). مجلة بيزنس ويك. مقال: «صُنَّاع البرامج ينساقون صوب نموذج الاشتراك».

Business Week,

<http://www.businessweek.com/articles/2013-11-14/2014-outlook-software-makers-subscription-drive>

90. ديفيد بوغ (17 سبتمبر 2013). مجلة ساينتيфик أميركان. مقال: «نموذج الاشتراك في برامج «أدوبي» يعني أنك لن تمتلك برمجياتك أبداً».

Scientific American,

<http://www.scientificamerican.com/article/adobe-software-subscription-modelmeans-you-cant-own-your-software>.

91. يمارس «غوغل» سياسة أفضل من غيره في مسألة نقل المستخدمين معلوماتهم معهم حينما يتركون خدماته.

92. هنري فاريل (خريف 2013). مجلة ديموقراطية العدد 30. «النخب الثقافية للتقنية».

Democracy 30,

<http://www.democracyjournal.org/30/the-tech-intellectuals.php>

93. ليس ذلك للقول إنَّ تلك الأشياء أساسية، وإنَّه من المستحيل الاستمرار من دونها. لا أملك حساباً على «فيسبوك». أعرف أشخاصاً لا يملكون هواتف خلوية، وهناك شخص لا يتسوق بواسطة الإنترنت إطلاقاً. لدينا خيار ما، لكن العيش من دون تلك الأشياء صعب تماماً، على المستويين الشخصي والمهني.

94. جيسيك غولدشتاين (24 إبريل 2014). مقال: «مقابلة مع امرأة بذلت قصارها كي تخفي حملها عن «البيانات الضخمة»».

Think Progress,

<http://thinkprogress.org/culture/2014/04/29/3432050/can-youhide-from-big-data>

الفصل 5: الرقابة والسيطرة الحكوميتان

1. بارتون غيلمان وأشكان سلطاني (14 أكتوبر 2013). صحيفة واشنطن بوست. مقال: «تجمع وكالة الأمن القومي» ملايين دفاتر العناوين في البريد الإلكتروني عالمياً.

Washington Post,

http://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-email-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story.html

- بارتون غيلمان وأشكان سلطاني (30 أكتوبر 2013). صحيفة واشنطن بوست. مقال: «وفق وثائق سنودن، تخترق وكالة الأمن القومي» روابط إلكترونية في مراكز بيانات «ياهو» و«غوغل» عالمياً.

Washington Post,

http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html

- بارتون غيلمان ولورا بواتراس (7 يونيو 2013). صحيفة واشنطن بوست، مقال: «الاستخبارات البريطانية والأمريكية تنقب في بيانات من 9 شركات للإنترنت، ضمن برنامج سري واسع».

Washington Post,

http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html.

2. توجيه تنفيذي من مكتب رئيس الولايات المتحدة (24 أكتوبر 1952). مذكرة إلى وزير الخارجية ووزير الدفاع: «وكالة استخباراتية للاتصالات»، «وكالة الأمن القومي للولايات المتحدة».

http://www.nsa.gov/public_info/_files/truman/truman_memo.pdf.

3. توماس بيرنز (1990). كتاب جذور وكالة الأمن القومي 1952-1940، عن «المركز الأمريكي لتاريخ التشفير»، «وكالة الأمن القومي».

http://www.nsa.gov/public_info/_files/cryptologic_histories/origins_of_nsa.pdf.

4. كتب علماء سياسة عن الفارق بين الأسرار والألغاز أو بين الألغاز والأحجيات. جوزيف س. ناي جونيور. مجلة فورين أفيرز. عدد (يوليو/أغسطس 1994). مقال: «التطلع إلى المستقبل».

Foreign Affairs,

<http://www.foreignaffairs.com/articles/50102/joseph-s-nye-jr/peering-into-the-future>

- جيوغري تريفتون (سبتمبر 2001). بحث: «إعادة هيكلة الاستخبارات القومية لتتلاءم مع عصر المعلومات». Research Brief 5, European Union Center for California, <http://eucenter.scrippscollege.edu/files/2011/06/Trevertan-05.pdf>.

5. دان غير (9 أكتوبر 2013). «مبادلات في الأمن السبراني». <http://geer.tinho.net/geer.uncc.9x13.txt>

6. بموجب قانون العام 1978 عن محكمة «فيسا» التي تنظم رقابة وكالة الأمن القومي، يفترض بالأشخاص المستهدفين داخل الولايات المتحدة أن يكونوا «عملاء دولة أجنبية». عندما عدل ذلك القانون في 2008، بات تعريف الهدف ينطبق على أي أجنبي.

7. دانا بريست (21 يوليو 2013). صحيفة واشنطن بوست. مقال: «تخفى نمو وكالة الأمن القومي» من الحاجة إلى استهداف إرهابيين».

Washington Post,

http://www.washingtonpost.com/world/national-security/nsa-growth-fueled-by-need-to-target-terrorists/2013/07/21/24c93cf4-f0b1-11e2-bed3-b9b6fe264871_story.html

8. فعلت الوكالة ذلك في 1984. ويليام ج. برود (8 نوفمبر 1998). صحيفة نيويورك تايمس. مقال: «قصة غواصة تجسس أمريكية شجاعة».

New York Times,

<http://www.nytimes.com/1998/11/08/us/a-tale-of-daring-american-submarine-espionage.html>

9. موقع «غوغل» (2014). «مواقع مراكز البيانات».

<https://www.google.com/about/datacenters/inside/locations/index.html>.

10. بارتون غيلمان وغريغ ميلر (29 أغسطس 2013). صحيفة واشنطن بوست. مقال: «نجاحات شبكة الجواسيس الأمريكيين وفشلها وأهدافها، تظهر تفصيلياً في «صندوق أسود» يلخص ميزانيتها».

Washington Post,

http://www.washingtonpost.com/world/national-security/black-budget-summary-details-us-spy-networks-successes-failures-and-objectives/2013/08/29/7e57bb78-10ab-11e3-8cdd-bcdc09410972_story.html

إيوين ماكأسكيل وجوناثان واتس (29 أغسطس 2013). صحيفة الغارديان. مقال: «مصدر سري رفيع يكشف أن إنفاق الاستخبارات الأمريكية تضاعف منذ 11/9».

Guardian,

<http://www.theguardian.com/world/2013/aug/29/us-intelligence-spending-double-9-11-secret-budget>

11. ريان سنغل (10 أكتوبر 2007). مجلة وايرد، «الاختراق المحظوظ لمصلحة وكالة الأمن القومي»: كيف تحولت أميركا إلى محوّل مفاتيح لمكالمات العالم».

Wired,

https://web.archive.org/web/20071019223411/http://www.wired.com/politics/security/news/2007/10/domestic_taps

كريستوفر ميمز (8 يونيو 2013). «لماذا تملك وكالة الأمن القومي» نفاذاً إلى 80 % من المكالمات الشبكية حتى من دون «الأبواب الخلفية» في محرّك «غوغل».

Quartz,

<http://qz.com/92369/why-nsa-has-access-to-80-of-online-communication-even-if-googledoesnt-have-a-back-door>.

12. إيوين ماكأسكيل وجيمس بول (2 نوفمبر 2013). صحيفة الغارديان. مقال: «بورتريه عن وكالة الأمن القومي»: لا هدف أصغر من أن يلاحظ، للتوصل إلى الرقابة الشاملة».

Guardian,

<http://www.theguardian.com/world/2013/nov/02/nsa-portrait-total-surveillance>.

غلين غرينوالد (2014). كتاب لا مكان للاختباء: إدوارد سنودن ووكالة الأمن القومي وحال الرقابة في الولايات المتحدة. (دار ماكميلان للنشر).

<http://leaksource.info/2014/07/31/glenn-greenwalds-no-place-to-hide-nsa-documents-excerpts>

13. بالطبع لا أعرف ذلك بصورة مؤكدة. وأورد بيل بليني، وهو مطلق صافرة إنذار آخر [كحال سنودن]، أن الوكالة تفعل ذلك، لكنه لم يقدم دليلاً على ذلك. أنطوني لوفينشتاين (10 يوليو 2014)، صحيفة الغارديان، مقال: «المقال النهائي لـ «وكالة الأمن القومي» هو السيطرة على الناس كلّهم».

Guardian,

<http://www.theguardian.com/commentisfree/2014/jul/11/the-ultimate-goal-of-thensa-is-total-population-control>

14. ريان ديفريه، غلين غرينوالد ولورا بواتراس (19 مايو 2014)، موقع «إنترسبت». مقال: «قراصنة البيانات في الكاريبي: وكالة الأمن القومي» تسجّل المكالمات الخلوية كافة في الدباهاماس».

Intercept,

<https://firstlook.org/theintercept/article/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas>

جوليان أسانج (23 مايو 2014)، «إعلان من «ويكيليكس» بصدد تسجيلات الهاتف الجماعية للأفغان، من قبل «وكالة الأمن القومي».

WikiLeaks,

<https://wikileaks.org/WikiLeaks-statement-on-the-mass.html>.

15. بارتون غيلمان وغريغ ميلر (29 أغسطس 2013). صحيفة واشنطن بوست. مقال: «نجاحات شبكة الجواسيس الأمريكيين وفشلها وأهدافها، تظهر تفصيلياً في «صندوق أسود» يلخص ميزانيتها».

Washington Post,

http://www.washingtonpost.com/world/national-security/black-budget-summary-details-us-spy-networks-successes-failures-and-objectives/2013/08/29/7e57bb78-10ab-11e3-8cdd-bcd09410972_story.html

16. دانا بريست (21 يوليو 2013)، واشنطن بوست، مقال: «تغذى نمو «وكالة الأمن القومي» من الحاجة لاستهداف إرهابيين».

Washington Post,

http://www.washingtonpost.com/world/national-security/nsagrowth-fueled-by-need-to-target-terrorists/2013/07/21/24c93cf4-f0b1-11e2-bed3-b9b6fe264871_story.html.

17. تذهب 70 % من ميزانية الاستخبارات إلى الشركات الخاصة، ويملك 483 ألف متعاقد تفويضات عالية السرية، ويمثلون 34 % من أصل 1.4 مليون شخص لديهم تفويضات على ذلك المستوى. روبرت أوهارو جونور، دانا بريست ومارجوري سنسر (10 يونيو 2013). صحيفة واشنطن بوست. «تسريبات «وكالة الأمن القومي» تظهر مدى اعتماد المؤسسة الاستخباراتية على متعاقدين خارجيين».

Washington Post,

http://www.washingtonpost.com/business/nsa-leaks-put-focus-onintelligence-apparatuss-reliance-on-outside-contractors/2013/06/10/e940c4ba-d20e-11e2-9f1a-1a7cdee20287_story.html.

Jonathan Fahey and Adam Goldman (10 Jun 2013),

«Leak highlights key role of private contractors», Associated Press,

<http://bigstory.ap.org/article/leak-highlights-key-role-private-contractors>

18. بارتون غيلمان وغريغ ميلر (29 أغسطس 2013). صحيفة واشنطن بوست. مقال: «نجاحات شبكة الجواسيس الأمريكيين وفشلها وأهدافها، تظهر تفصيلياً في «صندوق أسود» يلخص ميزانيتها».

Washington Post,

http://www.washingtonpost.com/world/national-security/black-budget-summary-details-us-spy-networks-successes-failures-and-objectives/2013/08/29/7e57bb78-10ab-11e3-8cdd-bcd09410972_story.html

19. ستيفن أفترغود (مارس 2014). بحث: «بيانات ميزانية الاستخبارات». «رابطة العلماء الأمريكيين - برنامج موارد الاستخبارات».

Federation of American Scientists Intelligence Resource Program,

<http://fas.org/irp/budget/index.html>

20. «نعتقد أن المهتمات العسكرية في العراق وأفغانستان تركت آثاراً يصعب قياسها لكنها ضخمة تماماً، في القرارات بشأن تقنيات جمع المعلومات وتقنيات الاتصالات». ريتشارد كلارك وآخرون (12 ديسمبر 2013)، «الحرية والأمن في عالم متغير: تقرير وتوصيات لجنة الرئاسة للمراجعة بشأن الاستخبارات وتقنيات الاتصالات»، المكتب التنفيذي للرئيس الأمريكي، ص 187.

http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

21. يُسميه المحققون الفيدراليون 12 ثلاث ثلاثات. المكتب التنفيذي للرئيس الأمريكي (4 ديسمبر 1981)، «الأمر التنفيذي رقم 12333 - بشأن نشاطات الاستخبارات الأمريكية». السجل الفيدرالي.
Federal Register,
<http://www.archives.gov/federal-register/codification/executive-order/12333.html>
الليكس أبدي (29 سبتمبر 2014). «وثائق جديدة تلقي الضوء على أقوى أدوات «وكالة الأمن القومي»». *Free Future*,
<https://www.aclu.org/blog/national-security/new-documents-shed-light-one-nsas-most-powerful-tools>
22. مارك جايكوكس (5 نوفمبر 2013). مؤسسة الحدود الإلكترونية. مقال: «3 تسريبات، 3 أسابيع وما الذي عرفناه عن السلطة التجسسية الأخرى للحكومة الأمريكية: الأمر التنفيذي 12333».
Electronic Frontier Foundation,
<https://www.eff.org/deeplinks/2013/10/three-leaks-three-weeks-and-what-weve-learned-about-governments-other-spying>
23. الكونغرس الأمريكي (2001). الفصل 215 من التشريع الأمريكي «باتريوت أكت».
<http://www.gpo.gov/fdsys/pkg/BILLS-107hr3162enr/pdf/BILLS-107hr3162enr.pdf>
24. 350 مارسي ويلر (14 أغسطس 2014). موقع «صالون». مقال: «الأبطال المزيّفون لجورج دبليو بوش: القصة الحقيقية للخداع السري في واشنطن».
Salon,
http://www.salon.com/2014/08/14/george_w_bushs_false_heroes_the_real_story_of_a_secret_washington_sham
25. هناك أيضاً «قانون حماية أميركا» للعام 2007. وجرى تجاوزه وإداله به التعديلات على قانون رقابة الاستخبارات الأجنبية، مع الاحتفاظ بمرجعية التخويلات التي يقدّمها «قانون حماية أميركا». لا نعلم عدد تلك التخويلات، ولا مدى أهميتها أيضاً. جيمس ريزين (6 أغسطس 2007). صحيفة نيويورك تايمس. مقال: «بوش يوقع قانوناً بتوسيع مدى التنصّت».
New York Times,
<http://www.nytimes.com/2007/08/06/washington/06nsa.html>
رايان سنغل (6 أغسطس 2007). مجلة وايرد. مقال: «تحليل: قانون جديد يمنح الحكومة 6 شهور كي تحوّل الإنترنت ونظم الهاتف، بنية دائمة للتجسس».
Wired,
<http://www.wired.com/2007/08/analysis-new-la>
26. تناقش إحدى وثائق سنودن إجراءات تقليصية للوكالة. «وكالة الأمن القومي» (8 يونيو 2007). «إجراءات تقليصية استخدمتها الوكالة في ما خصّ مصادرة معلومات ترجع لاستخبارات أجنبية، بالتوافق مع الفصل 702 من «قانون رقابة الاستخبارات الأجنبية» معذلاً». موقع صحيفة الغارديان.
<http://www.theguardian.com/world/interactive/2013/jun/20/exhibit-b-nsa-procedures-document>
27. جينيفر غرانيك (25 أغسطس 2014)، موقع «جاست سيكيوريتي»، مقال: «الإبلاغ عن اعتراض الاتصالات يطرح سؤالاً أوسع بخصوص تقليص البيانات الوصفية».
Jennifer Granick (25 Aug 2014), «Intercept reporting raises broader metadata minimization question»,
Just Security,
<http://justsecurity.org/14327/intercept-reporting-raises-broader-metadata-minimization-question>
Marcy Wheeler (26 Aug 2014), «SPCMA and ICREACH», *Empty Wheel*,
<http://www.emptywheel.net/2014/08/26/spcma-and-icreach>

28. بارتون غيلمان، جوليا تايبث وأشكان سلطاني (5 يوليو 2014)، صحيفة واشنطن بوست، مقال: «في بيانات اعتراض الاتصالات، تفوق أعداد غير المستهدفين بما لا يقاس أولئك المصنفين أهدافاً».
Washington Post,
http://www.washingtonpost.com/world/national-security/in-nsaintercepted-data-those-not-targeted-far-outnumber-the-foreigners-who-are/2014/07/05/8139adf8-045a-11e4-8572-4b1b969b6322_story.html
29. نادية كيالي (21 مايو 2014). موقع «غيزمودو». مقال: «كيف تغير وكالة الأمن القومي» إنفاذ القانون».
Gizmodo,
<http://gizmodo.com/how-the-nsa-istransforming-law-enforcement-1579438984>
30. رايان غلامار (25 أغسطس 2014). موقع «إنترسبت». مقال: «محرك الرقابة: كيف صنعت وكالة الأمن القومي» محرك بحثها السري المشابه لـ«غوغل».
Intercept,
<https://firstlook.org/theintercept/2014/08/25/icreach-nsa-cia-secret-google-crisscross-proton>
31. حدث التوسع الأكثر دلالة في سلطات «وكالة الأمن القومي» في العام 2005، تحت مظلة «قانون تحسين «قانون باتريوت» وإعادة هيكلة تخويلاته». ونظراً إلى بعض مواد ذلك القانون باعتبارها غير شرعية.
32. جون فيلانسور (30 ديسمبر 2013). مجلة «آتلانتك». مقال: «ماذا تعرف عن «مبدأ الطرف الثالث»؟»
Atlantic,
<http://www.theatlantic.com/technology/archive/2013/12/what-you-need-to-know-about-thethird-party-doctrine/282721>.
33. يختصر مصطلح «أي أم سي أي» عبارة «الهوية العالمية للمشارك في الهاتف النقال» (*International Mobile Subscriber Identity*). وتتمثل في رقم متسلسل متفرد يعطى لهاتفك لتمكينه من البث، فيعرف نظام شبكة الخلوي مكان وجودك.
34. الاسم الشيفري الآخر هو «أمبرجك» (*AmberJack*). حاضراً، يستعمل «ستنفراي» بوصفه اسم النوع لأدوات «أي أم أس أي» كاتشر».
35. جويل هروسكا (14 يونيو 2014). مجلة «إكسبريم تيك». «ستنفراي»: برج زائف للخلوي تستعمله الشرطة وشركات النقل لتتبعك في الأمكنة كافة».
Extreme Tech,
<http://www.extremetech.com/mobile/184597-stingray-the-fake-cell-phone-towercops-and-providers-use-to-track-your-every-move>.
36. لورين وولكر (23 سبتمبر 2014). مجلة «نيوزويك». مقال: «وثائق جديدة تكشف معلومات عن أدوات تعقب تستخدمها الشرطة».
Newsweek,
<http://www.newsweek.com/new-documents-reveal-information-about-police-cell-phone-tracking-devices-272746>
37. كيم زيت (19 يونيو 2014). مجلة «وايرد». مقال: «رسائل بريد إلكتروني تكشف أن الضباط الفيدراليين طلبوا من شرطة فلوريدا خداع القضاة».
Wired,
<http://www.wired.com/2014/06/feds-told-cops-to-deceive-courts-about-stingray>
38. ناثان فريد ويسلر (3 يونيو 2014). مجلة «فري فيوتشر» على موقع «الاتحاد الأمريكي للحريات المدنية».
«جنرالات أميركا الفيدراليون صادروا وثائق مكالمات هاتفية من بوليس محلي في محاولة استثنائية لمنع وصولها إلى الجمهور».
Free Future,
<https://www.aclu.org/blog/national-security-technology-and-liberty/us-marshals-seize-local-cops-cell-phone-tracking-files>.

Kim Zetter (3 Jun 2014), «U.S. Marshals seize cops' spying records to keep them from the ACLU», *Wired*,

<http://www.wired.com/2014/06/feds-seize-stingray-documents>

39. «المركز القومي لمكافحة الإرهاب» (2007). «مخزن بيانات هويات الإرهابيين وبيئتهم» [TIDE]. https://web.archive.org/web/20140712154829/http://www.nctc.gov/docs/Tide_Fact_Sheet.pdf

ريتشارد أ. بست جونيور (19 ديسمبر 2011)، «خدمة بحوث الكونغرس»، مقال: «المركز القومي لمكافحة الإرهاب»: المسؤوليات والقلق المحتمل للكونغرس.

Congressional Research Service,

<http://fas.org/sgp/crs/intel/R41022.pdf>

مات سليج (16 فبراير 2013). صحيفة هافنغتون بوست. مقال: «وثيقة عن بيانات الإرهابيين في المركز القومي لمكافحة الإرهاب».

Huff-ington Post,

http://www.huffingtonpost.com/2013/02/15/national-counterterrorism-center-nctc-terrorist-information_n_2697190.html

40. كارين دي يونغ (25 مارس 2007). صحيفة واشنطن بوست. «قاعدة بيانات الإرهابيين زادت بأربعة أضعاف في أربع سنوات».

Washington Post,

<http://www.washingtonpost.com/wp-dyn/content/article/2007/03/24/AR2007032400944.html>.

41. جوليا أنفونين (13 ديسمبر 2013). صحيفة وول ستريت جورنال. مقال: «وكالة أمريكية لمكافحة الإرهاب تمارس التنصت بواسطة قاعدة بيانات واسعة لمواطنين».

Wall Street Journal,

<http://online.wsj.com/news/articles/SB10001424127887324478304578171623040640006>

42. جيمي سكاويل وريان دينغفو (5 أغسطس 2014). موقع «انترسيبت». مقال: «قائد التجسس: النظام باراك أوباما السري لتتبع الإرهابيين بالأرقام».

Intercept,

<https://firstlook.org/theintercept/article/2014/08/05/watch-commander>

43. إريك شميدت ومايكل شميدت (24 إبريل 2013). صحيفة نيويورك تايمس. مقال: «اسم مفجر «ماراثون بوسطن» كان على قوائم وكالتين أمريكيتين».

New York Times,

<http://www.nytimes.com/2013/04/25/us/tamerlan-tsarnaev-bomb-suspect-wason-watch-lists.html>.

44. وزارة العدل الأمريكية (2014). «فرق العمل لدعم مكافحة الجريمة المنظمة». <http://www.justice.gov/criminal/taskforces/ocdetf.html>.

45. المكتب التنفيذي للرئاسة الأمريكية (2009). «المبادرة القومية الشاملة لأمن الفضاء السبراني». <http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative>

46. روبرت بوكهوسين (5 إبريل 2013). مجلة وايرد. مقال: «يسعى مكتب الكحول والتبغ والأسلحة النارية إلى صنع قاعدة بيانات «مكثفة» كي يعرف من هم أصدقاؤك».

Wired,

<http://www.wired.com/2013/04/atf-database>.

47. ليزا مايرز، دوغلاس باسترنكا وريتش غارديلا (14 ديسمبر 2005). شبكة «آن بي سي نيوز». مقال: «هل يتجسس البنتاغون على الأميركيين؟»

NBC News,

http://www.nbcnews.com/id/10454316/ns/nbc_nightly_news_with_brian_williams-nbc_news_investigates/t/pentagon-spying-americans

مارسي ويلر (24 يوليو 2007). مقال: «كانينغهام، سي أي أف إيه» وتشيني: رواية جديدة للتاريخ».

Empty Wheel,

<http://www.emptywheel.net/2007/07/24/cunningham-cifa-and-cheney-a-new-chronology>

48. في العام 2014، قرّرت محكمة فيدرالية أنّ تلك الممارسة ليست قانونية، وألغت إدانة بممارسة جنس أطفال إباحي، كانت مستندة إلى أدلة المكتب. فيكتوريا كافالير (18 سبتمبر 2014). وكالة «رويترز». مقال: «محكمة أميركية تخطئ ممارسة البحرية رقابة على الحواسيب في سياق تحقيق عن جنس أطفال إباحي».

Reuters,

<http://www.reuters.com/article/idUSKBN0HD2EU20140918>

49. روبرت مولر (15 نوفمبر 2004). موقع «إف بي أي». «الداف بي أي»: تحسين الاستخبارات من أجل أمريكا أكثر أمناً، خطاب في قاعة البلدية في مدينة «لوس أنجلوس».

<http://www.fbi.gov/news/speeches/the-fbi-improving-intelligence-for-a-safer-america>

«وزارة الأمن الوطني» (4 سبتمبر 2012). «منشورات عن مراكز الانصهار».

<http://www.dhs.gov/sites/default/files/publications/Fusion%20Centers%20Handout.pdf>

مجلس النواب الأمريكي (يوليو 2013). «تقرير موظفي الأغلبية عن شبكة وطنية لمراكز الانصهار»، لجنة «وزارة الأمن الوطني».

<http://homeland.house.gov/sites/homeland.house.gov/files/documents/CHS%20SLFC%20Report%202013%20FINAL.pdf>

50. تورين مناهان (2010). مجلة سوشال جستس. بحث: «مستقبل الأمن؟ عمليات الرقابة في مراكز الانصهار التابعة لوزارة الأمن الوطني».

Social Justice 37,

http://www.socialjusticejournal.org/archive/120_37_2-3/120_07Monahan.pdf.

51. بريسيلا م. ريفان، تورين مناهان وكريستا كرافن (3 ديسمبر 2013). «تركيب المشتبه فيه: إنتاج البيانات وتداولها وتفسيرها في «مراكز الانصهار» لوزارة الأمن الوطني».

Administration and Society,

<http://aas.sagepub.com/content/early/2013/11/29/0095399713513141.abstract>

52. ميتشل غيرمان وغاي ستانلي (ديسمبر 2013). «الاتحاد الأمريكي للحريات المدنية». «ما خطب مراكز الانصهار؟»

American Civil Liberties Union,

https://www.aclu.org/files/pdfs/privacy/fusioncenter_20071212.pdf.

شارون برادفورد فرانكلين وآخرون (6 سبتمبر 2012)، مؤسسة «مشروع الدستور». مقال: «توصيات إلى مراكز الانصهار: حماية الخصوصية والحريات المدنية في سياق الحماية من الجريمة والإرهاب».

Constitution Project,

<http://www.constitutionproject.org/pdf/fusioncenterreport.pdf>

53. كوان مونيهان (22 أيار 2014). صحيفة نيويورك تايمس. مقال: «رسميون نشروا شبكة واسعة لمراقبة حركة «احتلوا وول ستريت»».

New York Times,

<http://www.nytimes.com/2014/05/23/us/officials-cast-wide-net-in-monitoring-occupy-protests.html>

مارا فيرمهايدن هيلر وكارل ميسنيو (5 أيار 2014). مؤسسة «الشراكة لأجل عدالة مدنية». مقال: «خروجاً من الظلال: الدور الخفي لمراكز الانصهار في رقابة على «حركة احتلوا وول ستريت» والاحتجاج السلمي في الولايات المتحدة».

Partnership for Civil Justice,

<http://www.justiceonline.org/one-nation-under-surveillance/out-of-the-shadowspcfj-report.pdf>.

54. «الاتحاد الأمريكي للحريات المدنية» (سبتمبر 2013). «منفلت وغير موثوق: لا رقابة على إساءة استعمال الدوافع بي أي، السلطة».

<https://www.aclu.org/sites/default/files/assets/unleashed-and-unaccountable-fbi-report.pdf>.

روبرتو سكاليز (10 إبريل 2014). صحيفة بوسطن غلوب. مقال: «الاتحاد الأمريكي للحريات المدنية، يقاضي الدوافع بي أي»، أمام المدعي العام لدوتداشيف، وفق وثائق فرقة المهمة.

Boston Globe,

<http://www.boston.com/news/local/massachusetts/2014/04/10/aclu-sues-fbi-attorney-for-todashev-task-force-records/MYWzetzg75Zy3DIpLB1nyrO/story.html>

55. «الاتحاد الأمريكي للحريات المدنية» (24 أغسطس 2010). مقال: «وفق وثيقة جديدة: الفرق المشتركة لمكافحة الإرهاب، التابعة للدوافع بي أي» استهدفت نشطاء مسالمين بالمضايقة والمراقبة السياسية».

<http://aclu-co.org/new-documents-confirm-fbis-joint-terrorism-task-force-targets-peaceful-activists-for-harassment-political-surveillance>

كيفن كوزستيل (4 يوليو 2014)، موقع «ديسنتر»، مقال: «تقارير عن مراجعة من الفرق المشتركة لمكافحة الإرهاب، التابعة للدوافع بي أي» وضباط فيدراليين كبار، قضية تتعلق بنشطاء سياسيين عمرها 30 سنة».

Dissenter,

<http://dissenter.firedoglake.com/2014/07/04/fbi-jttf-us-marshalservice-are-reportedly-visiting-political-activists-about-thirty-year-old-case>

56. سينسر إكرمان (23 سبتمبر 2011). مجلة وايرد، مقال: «دليل جديد على تفكير معاد للإسلام، يثير تحذيرات عميقة حيال وعد الدوافع بي أي» بالإصلاح».

Wired,

<http://www.wired.com/2011/09/fbi-islam-domination/all>

57. 383 آدم غابات (1 أغسطس 2013). صحيفة الغارديان، مقال: «تفتيش منزل امرأة في نيويورك بعد أن بحثت في الإنترنت عن معلومات تتعلق بطنانجر الضفط».

Guardian,

<http://www.theguardian.com/world/2013/aug/01/new-york-police-terrorism-pressure-cooker>.

كارلوس ميلر (23 مايو 2014)، مقال: «بوليس من فرقة مكافحة الإرهاب يفتش منزل مصوّر التقط صوراً لمباني الشرطة».

Photography Is Not a Crime,

<http://photographyisnotacrime.com/2014/05/23/terrorist-task-force-cop-visits-man-home-photographing-police-buildings>.

ستيف أنير (11 يوليو 2014)، مجلة بوسطن مغازين، «رفع قضية من الاتحاد الأمريكي للحريات المدنية، ضد الشرطة، بعد فرضه رقابة على مصوّر بسبب «سلوك مريب»».

Boston Magazine,

<http://www.bostonmagazine.com/news/blog/2014/07/11/aclu-james-prigoff-terrorism-task-force-lawsuit>

58. دنكان كامبل (3 يونيو 2014). مقال: «الكشف عن مركز سريّ جداً لُتصّت على الإنترنت في الشرق الأوسط تابع لدالقيادة الحكومية للاتصالات».

Register,

http://www.theregister.co.uk/2014/06/03/revealed_beyond_top_secret_british_intelligence_middleeast_internet_spy_base.

59. نيكسي هاغر وستيفانيا موريزي (5 نوفمبر 2013). صحيفة لي سبريسو. مقال: «قبرص مقر أميركي / بريطاني مشترك للتجسس على الإنترنت في الشرق الأوسط».

L'Espresso,

<http://espresso.repubblica.it/inchieste/2013/11/04/news/the-history-of-british-intelligence-operations-in-cyprus-1.139978>.

ريتشارد نورتن تايلور (28 نوفمبر 2013). صحيفة الغارديان. مقال: «مذكرات سرية تظهر جهود جهاز إيم أي 5» و«إم أي 6» والقيادة الحكومية للاتصالات، للحفاظ على قبرص قاعدة لهم».

Guardian,

<http://www.theguardian.com/uk-news/2013/nov/29/intelligence-mi5-mi6-gchq-cyprusnational-archives>

60. سفن بيكر وآخرون (18 يونيو 2014). صحيفة دير شبيغل، مقال: «كشوفات جديدة عن وكالة الأمن القومي»: دواخل ملف ألمانيا».

Der Spiegel,

<http://www.spiegel.de/international/germany/newsnowden-revelations-on-nsa-spying-in-germany-a-975441.html>

هوبرت جود وآخرون (18 يونيو 2014). صحيفة دير شبيغل، مقال: «التجسس معاً: التعاون العميق بين ألمانيا ووكالة الأمن القومي».

Der Spiegel,

<http://www.spiegel.de/international/germany/the-german-bnd-and-americannsa-cooperate-more-closely-than-thought-a-975445.html>.

61. جاك فلورو وغلين غرينولد (21 أكتوبر 2013)، صحيفة لوموند، «فرنسا في مقعد مشترك مع وكالة الأمن القومي»: رقابة شبكات الهواتف».

Le Monde,

http://www.lemonde.fr/technologies/article/2013/10/21/france-in-the-nsa-s-crosshair-phone-networks-under-surveillance_3499741_651865.html.

جاك فلورو وفرانك جوهانس (4 يوليو 2013)، مجلة سوسيتيه، مقال: «كشوفات عن «الأخ الكبير» الفرنسي».

Société,

http://www.lemonde.fr/societe/article/2013/07/04/revelations-on-the-french-big-brother_3442665_3224.html

62. رايان غالامار (18 يوليو 2014). موقع «إنترسبت»، مقال: «كيف وسّع الشركاء السريون شبكة الصيد لوكالة الأمن القومي».

Intercept,

<https://firstlook.org/theintercept/article/2014/06/18/nsa-surveillance-secret-cable-partners-revealed-rampart-a>.

63. جاسون أوم (30 أكتوبر 2013). شبكة «إيه بي سي نيوز-أستراليا». مقال: «خبر في التجسس يشرح كيف عملت أستراليا» قاعدة تنصّ، لوكالات الاستخبارات الأميركية، وضمنها «وكالة الأمن القومي».

ABC News Australia,

<http://www.abc.net.au/news/2013-10-30/australia-acting-as-listening-post-for-us-spy-agencies/5056534>

64. غلين غرينولد وريان غالامار، موقع «إنترسبت»، مقال: «نيوزلندا أطلقت مشروعاً للرقابة العامة فيما أنكرته علانية».

Intercept,

<https://firstlook.org/theintercept/2014/09/15/new-zealand-gcsb-spear-gun-mass-surveillance>

65. كريغ تيمبرغ (6 يونيو 2014). صحيفة واشنطن بوست، مقال: «شركة «فودافون» تصرّح بأن الحكومات تجمع معلومات عن مواطنيها، من دون قيود».

Washington Post,

http://www.washingtonpost.com/business/technology/governments-collecting-personal-data-without-limit-says-vodafone/2014/06/06/ff0cfc1a-edb4-11e3-9b2d-114aded544be_story.html

66. مايكل آر. غوردن. (7 فبراير 2014). صحيفة نيويورك تايمز، مقال: «أندونيسيا تتهم أستراليا بالتتصت على المحادثات».

New York Times,

<http://www.nytimes.com/2014/02/18/world/asia/indonesia-takes-aim-at-australia-over-spying-but-not-the-us.html>.

67. 393 أندريه سولداتوف وإيرينا بوروغان (خريف 2013). مجلة ورلد بوليسي جورنال. بحث: «حال الرقابة في روسيا».

World Policy Journal,

<http://www.worldpolicy.org/journal/fall2013/Russia-surveillance>

جيمس أ. لويس (18 إبريل 2014). «مركز الدراسات الاستراتيجية العالمية». بحث: «ملاحظة مرجعية عن رقابة الاتصالات في روسيا».

Center for Strategic and International Studies,

<http://csis.org/publication/reference-note-russian-communications-surveillance>.

68. تسمى النسخة الأكثر حداثة من ذلك النظام «سورم 3»، وتجمع بيانات رقابة بالجملة عن كل نظم الاتصالات، مع امتلاك نفاذ إلى المعلومات الجارية والتاريخية معاً. أندريه سولداتوف وإيرينا بوروغان (21 ديسمبر 2012). مجلة وايرد. مقال: «في الجمهوريات السوفييتية السابقة، ما زال الجاسوس التقني يراقبك».

Wired,

<http://www.wired.com/2012/12/russias-hand/all>.

69. 395 أوين ماثيوز (12 فبراير 2014)، مجلة نيوزويك، مقال: «روسيا تختبر نظاماً لـالرقابة الشاملة، في دورة «سوتشي»».

Newsweek,

<http://www.newsweek.com/2014/02/14/russia-tests-total-surveillance-sochi-olympics-245494.html>

جوشوا كوبشتاين (13 فبراير 2014). صحيفة نيويورك. مقال: «الإرث الآخر لدورة «سوتشي»».

New Yorker,

<http://www.newyorker.com/tech/elements/sochis-other-legacy>.

70. غوس هوزين (2010). «منظمة الخصوصية الدولية». بحث: «الخصوصية بوصفها حقاً سياسياً».

Index on Censorship 39,

https://www.privacyinternational.org/reports/privacy-asa-political-right/surveillance-of-political-movements#footnote5_5pc3hb7.

71. جيمس أ. لويس (2006). «مركز الدراسات الاستراتيجية العالمية». بحث «هندسة السيطرة: الرقابة على الإنترنت في الصين».

Center for Strategic and International Studies,

http://csis.org/files/media/csis/pubs/0706_cn_surveillance_and_information_technology.pdf

72. صحيفة أستراليا (4 مارس 2011). مقال: «نقد نظام تتبع الهواتف في الصين بوصفه «رقابة الأخ الكبير»».

Australian,

<http://www.theaustralian.com.au/news/world/china-mobile-phone-tracking-system-attacked-as-big-brother-surveillance/story-e6frg6so-1226015917086>

73. فرانك لانغفيل (29 يناير 2013). مقال: «في الصين، كن حذراً: ربما هناك كاميرا تراقبك».

NPR Morning Edition,

<http://www.npr.org/2013/01/29/170469038/in-china-beware-a-camera-may-be-watching-you>

74. كالوم ماكلويد (3 يناير 2013). صحيفة يو إس داي توبي، مقال: «رقابة الصين تستهدف الجريمة... والمنشقين».

USA Today,
http://www.usatoday.com/story/news/world/2013/01/03/china-security/1802177

75. فيرنون سيلفر (8 مارس 2013). مجلة بلومبرغ بيزنس وويك. مقال: «اختراق نظام الرقابة الصيني على «سكايب»».

Bloomberg Business Week,
http://www.businessweek.com/articles/2013-03-08/skypes-been-hijacked-in-china-and-microsoft-is-o-dot-k-dot-with-it

76. جون ماركوف (1 أكتوبر 2008). صحيفة نيويورك تايمس. مقال: «هناك رقابة على برنامج «سكايب» في الصين».

New York Times,
http://www.nytimes.com/2008/10/02/technology/internet/02skype.html

77. جون روبينو (13 يناير 2011). مقال: «شركة «آر. إي. أم» [صانعة هواتف «بلاك بيري»] تسمح للهند بالوصول إلى رسائل مستخدمي «بلاك بيري»».

John Ribeiro (13 Jan 2011), «RIM allows India access to consumer BlackBerry messaging», CIO,
http://www.cio.com/article/654438/RIM_Allows_India_Access_to_Consumer_BlackBerry_Messaging.

أمول شارما (28 أكتوبر 2011). صحيفة وول ستريت جورنال. مقال: «شركة «آر. إي. أم» تساعد جهود الهند في الرقابة».

Wall Street Journal,
http://online.wsj.com/news/articles/SB10001424052970204505304577001592335138870.

78. ألكساي أنيششوك (25 إبريل 2011). وكالة رويترز للأخبار. مقال: «شركة «بلاك بيري» تسعى إلى «التوازن» في روسيا».

Reuters,
http://www.reuters.com/article/2011/04/25/us-blackberry-russia-idUSTRE73012L20110425

79. قناة الجزيرة، التلفزيونية. (4 أغسطس 2010). مقال: «السعودية تحظر «بلاك بيري» بداية من يوم الجمعة».

AlJazeera,
http://www.aljazeera.com/news/middleeast/2010/08/2010844243386999.html

80. صحيفة جاكارتا بوست (15 سبتمبر 2011). مقال: «الحكومة تطلب من شركة «آر. أي. إم» نفاذاً مفتوحاً كي تتنصت على مستخدمي «بلاك بيري»».

Jakarta Post,
http://www.thejakartapost.com/news/2011/09/15/government-asks-rim-open-access-wiretap-blackberry-users.html

81. جوش هاليداي (18 إبريل 2011). صحيفة الغارديان. مقال: «دولة الإمارات العربية المتحدة تشدد القيود على «بلاك بيري»».

Guardian,
http://www.theguardian.com/technology/2011/apr/18/uae-blackberry-mails-secure

82. آر. جاي كريشنا (8 أغسطس 2012). صحيفة وول ستريت جورنال. مقال: «الهند تقترح اتفاقية للخلاف مع «بلاك بيري»».

Wall Street Journal,

<http://online.wsj.com/news/articles/SB10000872396390443404004577576614174157698>

«هيئة الإنذاعة البريطانية» (11 يوليو 2013). مقال: «الهند «متأهبة لاستعمال» نظام لاعتراض رسائل «بلاك بيرى»».

BBC News,

<http://www.bbc.com/news/technology-23265091>.

83. جيمس بول وبينجامين غوتليب (25 سبتمبر 2012). صحيفة الغارديان. مقال: «إيران تشدد الرقابة على الإنترنت بصنع شبكة خاصة بها».

Guardian,

<http://www.theguardian.com/world/2012/sep/25/iran-state-run-internet>

84. آنش. جي. أولبريخت (2003). بحث: «أولبريخت 2003: الحقيقة والكفاءة القانونيتين لعمليات اعتراض الاتصالات التي يشار إليها باسمي «100 أ» و«100 ب إس تي بي أو» وغيرها من إجراءات التحقيق: خلاصة». «معهد ماكس بلانك لقانون الجرائم الدولي والخارجي».

http://www.gesmat.bundesgerichtshof.de/gesetzesmaterialien/16_wp/telekueberw/rechtswirklichkeit_20abschlussbericht.pdf.

85. ونستون ماكسويل وكريستوفر وولف (23 مايو 2012). بحث: «حقيقة عالمية: نفاذ الحكومات إلى البيانات في السُّحْب الرقمية: دراسة مقارنة لعشرة نُظُم قانونية دولية».

Hogan Lovells,

http://www.cil.cnr.fr/CIL/IMG/pdf/Hogan_Lovells_White_Paper_Government_Access_to_Cloud_Data_Paper_1.pdf.

86. «هيئة الإنذاعة البريطانية» (20 نوفمبر 2012). أخبار «بي بي سي». مقال: «امرأة هندية مصدومة لاعتقالها بسبب تدوينة على «فيسبوك»».

BBC News,

<http://www.bbc.com/news/world-asiaindia-20405457>.

«وكالة الأنباء الفرنسية» (19 نوفمبر 2012). صحيفة ساوث شاينا مورنينغ بوست. مقال: «اعتقال هنود إثر تدوينات على «فيسبوك» عن إضراب مومباي».

Agence France-Presse (19 Nov 2012), «Indians arrested for Facebook post on Mumbai shutdown», *South China Morning Post*,

<http://www.scmp.com/news/asia/article/1086094/indians-arrested-facebook-post-mumbai-shutdown>.

87. ديفيد ستوت (9 يوليو 2014). مجلة تايم. مقال: «الطفمة العسكرية الحاكمة في تايلاند تعتقل مدرّساً بسبب تعليق على «فيسبوك»».

Time,

<http://time.com/2968680/thailand-juntaeditor-facebook-thanapol-eawsakul-fah-diew-khan>

88. «شبكة آسيا نيوز» (4 يونيو 2013). صحيفة ستار تريس تايمس. مقال: «اعتقال امرأة بسبب تدوينة على «فيسبوك» عُدت مسيئة للملك الماليزيا».

<http://news.asiaone.com/News/Latest+News/Science+and+Tech/Story/A1Story20130604-427357.html>

89. من المحتمل أن حكومة أخرى كانت وراء الاختراق الأصلي، وأن الإيرانيين امتطوا سطح ذلك النجاح. هانز هونغزستراتن وآخرون (13 أغسطس 2012). شركة «فوكس آي تي» مقال: «الدتوليب» الأسود: تقرير عن اختراق «سلطة «ديجيتال» للمصادقة».

<http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2012/08/13/black-tulip-update/black-tulip-update.pdf>.

90. سوميني سانغوبتا (11 سبتمبر 2011). صحيفة نيويورك تايمس. مقال: «هاكر» يهز دوائر الأمن».

<http://www.nytimes.com/2011/09/12/technology/hacker-rattles-internet-security-circles.html>.

91. كريغ غايزر (6 سبتمبر 2011). مجلة عالم الكمبيوتر. مقال: «تجسس هكرز» على 300 ألف عنوان بريد إلكتروني إيراني في «جي ميل» باستخدام مصادقة مزيفة من «غوغل».

Computer World,

http://www.computerworld.com/s/article/9219731/Hackers_spied_on_300_000_Iranians_using_fake_Google_certificate.

92. «مرصد أسلحة المعلوماتية». جامعة تورنتو، «مختبر المواطن»، «مركز مونك للدراسات الدولية». بحث: «تتبع غوست نت»: تحقيق عن شبكة تجسس سبراني».

<http://www.infowar-monitor.net/ghostnet>.

93. إلين ناكاشيما (28 مايو 2012). صحيفة واشنطن بوست. مقال: «فيروس كومبيوتر يستخدم للتجسس، ويفوق فيروس «ستاكس نت» بعشرين ضعفاً».

Washington Post,

http://www.washingtonpost.com/world/national-security/newly-identified-computer-virus-used-for-spying-is-20-times-size-of-stuxnet/2012/05/28/gJQAWa3VxU_story.html.

94. دان غودين (14 يناير 2013). موقع «آرس تكنيكا». مقال: «برنامج خبيث للتجسس المكثف استمر في التجسس على الحكومات بخفاء لـ 5 سنوات».

Ars Technica,

<http://arstechnica.com/security/2013/01/red-Oct-computer-espionage-network-may-have-stolen-terabytes-ofdata>

95. بيتر آيس وجيم فينكل (7 مارس 2014). وكالة «رويترز» للأنباء. مقال: «برنامج تجسس روسي اسمه «تورلا»، استهدف أوروبا والولايات المتحدة».

Reuters,

<http://www.reuters.com/article/2014/03/07/us-russia-cyberespionage-insight-idUSBREA260YI20140307>

96. مختبر شركة «كاسبارسكي» (10 فبراير 2014). «إمالة اللثام عن «كاريتو»: فيروس التطبيقات المفتوح».

Securelist,

http://www.securelist.com/en/downloads/vlpdfs/unveilingthemask_v1.0.pdf

97. إلين ناكاشيما (29 مايو 2014). صحيفة واشنطن بوست. مقال: «هكرز» إيرانيون استهدفوا رسميين أميركيين».

Washington Post,

http://www.washingtonpost.com/world/national-security/iranian-hackers-are-targeting-us-officials-through-social-networksreport-says/2014/05/28/7cb86672-e6ad-11e3-8f90-73e071f3d637_story.html

98. ماثيو م. إيد (10 يونيو 2013). مجلة فورين بوليسي. مقال: «في دواخل المجموعة الأشد سرية في وكالة الأمن القومي» لاختراق الصين».

Foreign Policy,

http://www.foreignpolicy.com/articles/2013/06/10/inside_the_nsa_s_ultra_secret_china_hacking_group.

99. بروس شنابر (4 أكتوبر 2013). صحيفة الغارديان. مقال: «الهجوم على برنامج «تور»: كيف استهدفت وكالة الأمن القومي» إخفاء الهوية لمستخدمي الإنترنت».

Guardian,

<http://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity>

100. الأسماء الشيفرية لتلك البرامج مسلية تماماً. وما يثير أشد الاهتمام أن تلك الوثيقة العالية السرية لوكالة

الأمن القومي»، لم تأت من إدوارد سنودن. موقع «لييك سورس» (30 ديسمبر 2013). وثيقة: «دليل إرشادي من قسم مكافحة الإرهاب» في «وكالة الأمن القومي» يظهر كيفية استغلال معظم البرمجيات الرقمية الكبرى، وكذلك الحال بالنسبة للمكونات الإلكترونية وبرمجيات الشركات.

<http://leaksource.info/2013/12/30/nsas-ant-division-catalog-of-exploits-for-nearly-every-major-software-hardware-firmware>

صحيفة دير شبيغيل (29 ديسمبر 2013). مقال: «دواخل مجموعة «تاو»: وثيقة تكشف المجموعة الأكثر تقدماً في اختراق الكمبيوتر لدى «وكالة الأمن القومي».

Der Spiegel,

<http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969.html>.

جاكوب أبلباوم، جوديث هورشيرت وكريستيان ستوكر (29 ديسمبر 2013). صحيفة دير شبيغيل، مقال: «تسوّق خدمة لأداة تجسس: كاتالوغ يشرح صندوق العدة عند «وكالة الأمن القومي»».

Der Spiegel,

<http://www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html>.

101. ماثيو م. آيد (15 أكتوبر 2013). مجلة فورين بوليسي. مقال: «محطمو الشيفرة الجدد لدى «وكالة الأمن القومي»».

Foreign Policy,

http://www.foreignpolicy.com/articles/2013/10/15/the_nsa_s_new_codebreakers

102. يتضمن المقال التالي وصفاً لإحدى الوحدات الصينية العسكرية لاختراق الكمبيوتر. ماندينت (18 فبراير 2013). مقال: «إي بي تي 1: عرض لإحدى أضخم وحدات التجسس السبراني في الصين».

http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

103. كيم زيت (13 يناير 2010). مجلة وايرد. مقال: «مخترقو نظام «غوغل» استهدفوا شيفرة المصدر في ما يزيد على 30 شركة».

Wired,

<http://www.wired.com/2010/01/google-hack-attack>

104. غريغ ويستون (16 فبراير 2011). شبكة «سي بي سي نيوز». مقال: «الحكومة الكندية استهدفها «هاكرز» أجانب».

CBC News,

<http://www.cbc.ca/news/politics/foreign-hackers-attack-canadian-government-1.982618>

105. نيكول براروت (31 يناير 2013). صحيفة نيويورك تايمس. مقال: «مجموعة «هاكرز» من الصين هاجمت نيويورك تايمس خلال الشهور الـ 4 الماضية».

New York Times,

<http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html>.

106. ألين ناكاشيما (19 مايو 2014). صحيفة واشنطن بوست. مقال: «الولايات المتحدة تعلن أول تهمة ضد بلد أجنبي بصدد التجسس السبراني».

Washington Post,

http://www.washingtonpost.com/world/national-security/us-to-announce-first-criminal-charges-against-foreign-country-for-cyberspying/2014/05/19/586c9992-df45-11e3-810f-764fe508b82d_story.html

107. ريفاريتشموند (2 أبريل 2011). صحيفة نيويورك تايمس. «كيف تمكّن الهاكرز» من اختراق شركة «آر أس إيه».

<http://bits.blogs.nytimes.com/2011/04/02/the-rsahack-how-they-did-it>.

Kelly Jackson Higgins (29 Mar 2012), «China hacked RSA, U.S. official says»,

Information Week,

<http://www.darkreading.com/attacks-breaches/china-hacked-rsa-us-official-says/d/d-id/1137409>

108. جوليان إي. بارنز (4 مارس 2008). صحيفة لوس أنجلوس تايمس. مقال: «البنتاغون قلق من نشاطات الصين في اختراق الكمبيوتر».

Los Angeles Times,

<http://articles.latimes.com/2008/mar/04/world/fg-uschina4>

ألين ناكاشيما (17 مايو 2013). صحيفة واشنطن بوست. مقال: «تقرير سري يعدّ نظم التسليح الأمريكية التي اخترقها جواسيس الفضاء السبراني الصينيون».

Washington Post,

http://www.washingtonpost.com/world/national-security/confidential-report-lists-us-weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1cc2dd-11e2-8c3b-0b5e9247e8ca_story.html.

109. لا نعترف إن كانت الحكومة الصينية تقف وراء تلك البرمجيات، لكن الحثثيات المرافقة لها تبدو كافية للإدانة. أندري غرينبرغ (1 أبريل 2013). مجلة فوربس. مقال: «أدلة متراكمة عن وقوف «هاكرز» الحكومة الصينية وراء برمجيات خبيثة في هواتف «أندرويد»».

Forbes,

<http://www.forbes.com/sites/andygreenberg/2013/04/01/evidencemounts-that-chinese-government-hackers-spread-android-malware>

110. ألين ناكاشيما وليزا راين (11 يوليو 2014). صحيفة واشنطن بوست. مقال: «اختراق صيني يستهدف بيانات موظفين حكوميين أمريكيين».

Washington Post,

http://www.washingtonpost.com/world/national-security/chinese-hackers-go-after-us-workers-personaldata/2014/07/10/92db92e8-0846-11e4-8a6a-19355c7e870a_story.html

111. بيتر شفائيزر (يناير/فبراير 1996). مجلة فورين آفيرز. مقال: «تصاعد التجسس الاقتصادي: أميركا هي الهدف رقم 1».

Foreign Affairs,

<http://www.foreignaffairs.com/articles/51617/peter-schweizer/the-growth-of-economic-espionageamerica-is-target-number-one>.

112. ديفيد سانغر (20 مايو 2014). صحيفة نيويورك تايمس. مقال: «عبر تهم بالتجسس، الولايات المتحدة تشدّ خيطاً مرهقاً ضدّ التجسس الصيني».

New York Times,

<http://www.nytimes.com/2014/05/20/us/us-treads-fine-line-in-fighting-chinese-espionage.html>.

جاك غولد سميث (25 مايو 2013). مجلة لو فاير. مقال: «سبب وهن الاتهام الأمريكي للصين بالتجسس». Jack Goldsmith (25 Mar 2013), «Why the USG complaints against Chinese economic cyber-snooping are so weak,» *Lawfare*,

<http://www.lawfareblog.com/2013/03/why-the-usg-complaints-against-chinese-economic-cyber-snooping-are-so-weak>.

113. صحيفة أو غلوبو (8 سبتمبر 2013). مقال: «وثائق «وكالة الأمن القومي» تظهر تجسساً أمريكياً على عتلاق النفط البرازيلي».

O Globo,

<http://g1.globo.com/fantastico/noticia/2013/09/nsa-documents-show-united-states-spied-brazilian-oil-giant.html>

114. صحيفة دير شبيغيل (15 سبتمبر 2013). مقال: «تتبع المال: وكالة الأمن القومي» تتجسس على نظام «سويقت» للمعاملات المالية العالمية.

Der Spiegel,

<http://www.spiegel.de/international/world/spiegel-exclusive-nsa-spies-on-international-bank-transactions-a-922276.html>

115. كينيث ديليو دام وهيربرت لين، كتاب دور التشفير في تأمين معلومات المجتمع (1996). (دار «ناشيونال أكاديميز برس»).

http://www.nap.edu/catalog.php?record_id=5131.

116. مورغان-ماركيز بوار وآخرون (24 يونيو 2014). جامعة تورنتو، «مختبر المواطن»، «مركز مونك للدراسات الدولية». مقال: «قصة بوليسية: برنامج خبيث للتجسس الحكومي صنعته 'هاكينغ تيم'».

Citizen Lab, Munk School of Global Affairs, University of Toronto,

<https://citizenlab.org/2014/06/backdoor-hacking-teams-tradecraft-android-implant>.

William Anderson (24 Jun 2014), «Hacking Team 2.0: The story goes mobile», Securelist, <http://securelist.com/blog/research/63693/hackingteam-2-0-the-story-goes-mobile>

117. بيل ماركزك وآخرون. (12 فبراير 2014). جامعة تورنتو، «مختبر المواطن»، «مركز مونك للدراسات الدولية». مقال: «شركة 'هاكينغ تيم' واستهداف الصحافيين الإثيوبيين».

<https://citizenlab.org/2014/02/hacking-team-targeting-ethiopian-journalists>

كريغ تيمبرغ (12 فبراير 2014). صحيفة واشنطن بوست. مقال: «نظم حكم أجنبية تستخدم برمجيات تجسس على الصحافيين، حتى في الولايات المتحدة».

Washington Post,

http://www.washingtonpost.com/business/technology/foreign-regimes-use-spyware-against-journalistseven-in-us/2014/02/12/9501a20e-9043-11e3-84e1-27626c5ef5fb_story.html

118. آندرو جاكوبس، مغويل ميلفت وجون ماركوف (13 يونيو 2010). صحيفة نيويورك تايمس. مقال: «غول» يحدّد مصدر الهجمات، ويهدّد بمغادرة الصين».

New York Times,

<http://www.nytimes.com/2010/01/13/world/asia/13beijing.html>

ديفيد إي. سانغر (6 مايو 2013). صحيفة نيويورك تايمس. مقال: «الولايات المتحدة تلقي باللوم مباشرة على الجيش الصيني بخصوص هجمات في الفضاء السبراني».

New York Times,

<http://www.nytimes.com/2013/05/07/world/asia/us-accuses-chinas-military-incyberattacks.html>

119. صحيفة نيويورك تايمس (7 مايو 2013). افتتاحية: «الصين والحرب السبرانية».

New York Times,

<http://www.nytimes.com/2013/05/08/opinion/china-and-cyberwar.html>.

ديفيد سانغر وإليزابيث بوميللر (31 مايو 2011). صحيفة نيويورك تايمس. مقال: «البنغاون سيصنّف هجمات الفضاء السبراني أفعالاً حربية».

New York Times.

<http://www.nytimes.com/2011/06/01/us/politics/01cyber.html>.

120. باراك أوباما (17 يناير 2014). صحيفة نيويورك تايمس. مقال: «خطاب أوباما عن تجسس وكالة الأمن القومي» على الهواتف.

New York Times,

<http://www.nytimes.com/2014/01/18/us/politics/obamas-speech-on-nsa-phone-surveillance.html>.

121. مايكل س. سميث، كيث برادشير وكريستين هاوزر (8 أكتوبر 2012). صحيفة نيويورك تايمز. مقال: «لجنة أمريكية تجد مخاطر في معذات صينية».
<http://www.nytimes.com/2012/10/09/us/us-panel-calls-huawei-and-zte-national-security-threat.html>
122. «وكالة الأمن القومي» (24 يونيو 2008). وثيقة: «سوفلثرو: بيانات المنتج عن مجس «إيه أن تي» اللاسلكي».
<http://leaksource.files.wordpress.com/2013/12/nsa-ant-souffletrough.jpg>
 «وكالة الأمن القومي» (24 يونيو 2008). وثيقة: «فيد-ثرو: بيانات المنتج عن مجس «إيه أن تي» اللاسلكي».
<http://leaksource.files.wordpress.com/2013/12/nsa-ant-feedthrough.jpg>
 «وكالة الأمن القومي» (24 يونيو 2008). وثيقة: «جيت بلو: بيانات المنتج عن مجس «إيه أن تي» اللاسلكي».
<http://leaksource.files.wordpress.com/2013/12/nsa-ant-jetplow.jpg>
 «وكالة الأمن القومي» (24 يونيو 2008). وثيقة: «هيد ووتر: بيانات المنتج عن مجس «إيه أن تي» اللاسلكي».
<http://leaksource.files.wordpress.com/2013/12/nsa-ant-headwater.jpg>
 «وكالة الأمن القومي» (24 يونيو 2008). وثيقة: «هالوكس ووتر: بيانات المنتج عن مجس «إيه أن تي» اللاسلكي».
<http://leaksource.files.wordpress.com/2013/12/nsa-ant-halluxwater.jpg>
123. جيرمي هسو (26 مارس 2014). مقال: «شكوك الولايات المتحدة بدعوى» الصينية تستند أساساً إلى الخدع التي تمارسها «وكالة الأمن القومي» نفسها».
IEEE Spectrum,
<http://spectrum.ieee.org/tech-talk/computing/hardware/us-suspicious-of-chinas-huawei-based-partly-on-nas-own-spy-tricks>
124. في التعابير العسكرية، يسمّى الاختراق بهدف التجسس «تسلل إلى شبكة كومبيوتر من الخارج»، ويختصر بمصطلح «سي أن إي» (CNE)، ويسمّى الاختراق بهدف إلحاق ضرر بالكومبيوتر «هجوم على شبكة حواسيب»، ويختصر بمصطلح «سي أن إيه» (CNA). ألكسندر كليمرغ وهيلي تيرما-كلار (15 أبريل 2011). دراسة: «الأمن السراني والقوة السرانية: المفاهيم والشروط والقدرات بهدف التعاون للعمل داخل «الاتحاد الأوروبي»».
- Directorate-General for External Policies of the Union,
[http://www.europarl.europa.eu/RegData/etudes/etudes/join/2011/433828/EXPO-SEDE_ET\(2011\)433828_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/etudes/join/2011/433828/EXPO-SEDE_ET(2011)433828_EN.pdf)
 Alexander Klimburg (2 Sep 2014), «Shades of cyber grey: Espionage and attack in cyberspace», *Fletcher Forum of World Affairs*,
<http://www.fletcherforum.org/2014/09/02/klimburg>
125. ولكن ذلك لا يمثل «حرباً سرانية»، على الرغم من شيوع استعمال ذلك المصطلح في الخطاب السياسي. لتجنّب الخلط بين الأمرين، يمكن قراءة الكتاب التالي: الحرب السرانية لن تحدث أبداً (2013)، تأليف: توماس ريد، «مطبعة جامعة أوكسفورد».
- <http://thomasrid.org/no-cyber-war>
126. جيمس بامفورد (13 أغسطس 2014). مجلة وايرد. مقال: «إدوارد سنودن: القصة غير المعلنة».
Wired,
<http://www.wired.com/2014/08/edward-snowden>
127. يملك عدد أكبر من البلدان قدرات في الحرب السرانية. كلية السياسة العامة في «جامعة جورج ماسون» (فبراير 2014). دراسة: «أسواق تصدير الأمن السراني». «شراكة فرجينيا للتنمية الاقتصادية».
<http://exportvirginia.org/wp-content/uploads/2014/02/Report-on-Cyber-Security-Preface.pdf>
128. جوشوا ديفيز (21 أغسطس 2007). مجلة وايرد. مقال: «الدعوى» يضرّيون البلد الأكثر اتّصلاً بالإنترنت في أوروبا».

https://web.archive.org/web/20071019223411/http://www.wired.com/politics/security/magazine/15-09/ff_estonia

129. جون ماركوف (13 أغسطس 2008). صحيفة نيويورك تايمس. مقال: «الهجمات السبرانية سبقت الحرب الفعلية».

New York Times

<http://www.nytimes.com/2008/08/13/technology/13cyber.html>.

130. ماثيو ويبفر (8 يوليو 2009). صحيفة الغارديان. مقال: «هجمات سبرانية تستهدف كوريا الجنوبية والولايات المتحدة».

Guardian,

<http://www.theguardian.com/world/2009/jul/08/south-korea-cyber-attack>

131. تشارلز كلوفر (11 مارس 2009). صحيفة فايننشال تايمس. مقال: «مجموعة يساندها الكرملين مسؤولة عن الهجمات السبرانية على أستراليا».

Financial Times,

<http://www.ft.com/cms/s/0/57536d5a-0ddc-11de-8ea3-0000779fd2ac.html>

132. مجلة كومبيوتر ويكلي (13 مارس 2009). مقال: «صغار السن مسؤولون عن هجمات أستراليا».

Computer Weekly,

<http://www.computerweekly.com/news/2240088733/Kids-responsible-for-Estonia-attack>

133. ديفيد كوشنر (26 فبراير 2013). مقال: «القصة الحقيقية لـ«ستاكس نت»».

IEEE Spectrum,

<http://spectrum.ieee.org/telecom/security/the-realstory-of-stuxnet>

كيم زيت (2014). كتاب العد العكسي لليوم صفر: «ستاكس نت» وإطلاق أول سلاح رقمي في العالم. دار «كراون بابليشرز».

<http://books.google.com/books/?id=iBTpnQEACAAJ>.

134. ويليام جي. برود، جون ماركوف وديفيد ي. سانغر (15 يناير 2011). صحيفة نيويورك تايمس. مقال: «تجربة إسرائيلية على دودة إلكترونية أدت لتأخير في برنامج إيران النووي».

New York Times,

<http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html>

135. نيكول بيلاروت (23 أكتوبر 2012). صحيفة نيويورك تايمس. مقال: «في الهجوم السبراني على «أرامكو»، الولايات المتحدة رأت ردًا إيرانيًا».

New York Times,

<http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html>.

وكالة أنباء «رويترز» (9 ديسمبر 2012). صحيفة نيويورك تايمس. مقال: «شركة «أرامكو» تقول إن هجوماً سبرانياً استهدف إنتاجها».

New York Times,

<http://www.nytimes.com/2012/12/10/business/global/saudi-aramco-says-hackers-took-aim-at-its-production.html>

136. دريك س. ريفرون. (صيف 2008). بحث: «مكافحة الإرهاب والتعاون الاستخباراتي». مجلة التغيير العالمي والحوكمة العدد 1.

<http://www.globalaffairsjournal.com/archive/Summer08/REVERON.pdf>.

137. روس أندرسون (-23 24 يونيو 2014). جامعة بنسلفانيا. بحث: «الخصوصية في مواجهة رقابة الحكومة: تقابل آثار الشبكة مع خيار الناس».

13th Annual Workshop on the Economics of Information Security, Pennsylvania State University,

<http://weis2014.econinfosec.org/papers/Anderson-WEIS2014.pdf>.

138. نيك بيرى وبيايزلي دودز (16 يوليو 2013)، وكالة «أسوشيتد برس»، مقال: «تحالف الأمم الخمسة كان محورياً في الأذى الذي سببته التبريات».

Associated Press,

<http://bigstory.ap.org/article/expertssay-us-spy-alliance-will-survive-snowden>.

139. هنريك مولتكه وغياردنغ (4 نوفمبر 2013). مقال: «الدانمارك جزء من الحلقة الداخلية لوكالة الأمن القومي».

Information,

<http://www.information.dk/477405>

140. مجلة دير شبيغل (22 يوليو 2013). مقال: «شركاء أساسيين: تحالف محوري بين ألمانيا والولايات المتحدة».

Der Spiegel,

<http://www.spiegel.de/international/world/german-intelligence-worked-closely-with-nsa-on-data-surveillance-a-912355.html>

هربرت غوديه وآخرون. (18 يونيو 2014). صحيفة دير شبيغل. مقال: «لنتجسس معاً: التعاون العميق بين ألمانيا ووكالة الأمن القومي».

Der Spiegel,

<http://www.spiegel.de/international/germany/thegerman-bnd-and-american-nsa-cooperate-more-closely-than-thought-a-975445.html>

141. إيوين ماكأسكل وجيمس بول (2 نوفمبر 2013). صحيفة الغارديان. مقال: «بورتريه عن وكالة الأمن القومي»: لا هدف أصغر من أن يلاحظ، للتوصل إلى الرقابة الشاملة».

<http://www.theguardian.com/world/2013/nov/02/nsa-portrait-total-surveillance>.

142. جاي سولون وسيويهان غورمان (9 مايو 2012). صحيفة وول ستريت جورنال. مقال: «خلف إحباط مخطط الطائرة النفاثة».

Wall Street Journal,

<http://online.wsj.com/news/articles/SB10001424052702304543904577394373945627482>

غلين غرينوالد ومرضى حسين (25 يوليو 2014). موقع «إنترسيبت». مقال: «شريك جديد لوكالة الأمن القومي».

Intercept,

<https://firstlook.org/theintercept/2014/07/25/nsas-new-partner-spying-saudi-arabias-brutal-state-police>

143. إدوارد سنودن (7 مارس 2014). «بيان إلى برلمان الاتحاد الأوروبي».

European Parliament,

<http://www.europarl.europa.eu/document/activities/cont/201403/20140307ATT80674/20140307ATT80674EN.pdf>.

144. آندي مولر ماكفون وآخرون (31 أغسطس 2014). صحيفة دير شبيغل. مقال: «صدقة بوجه مزدوج: تركيا هي «الشريك والهدف» بالنسبة لوكالة الأمن القومي».

Der Spiegel,

<http://www.spiegel.de/international/documents-show-nsa-and-gchq-spied-on-partner-turkey-a-989011.html>.

لورا بواتراس وفريقها (31 أغسطس 2014). موقع «إنترسيبت». مقال: «كيف ساعدت وكالة الأمن القومي تركيا في قتل المتمردين الأكراد».

Intercept,

<https://firstlook.org/theintercept/2014/08/31/nsaturkeysiegel>

145. ديفيد إي. سانغر (1 مايو 2014). صحيفة نيويورك تايمس. مقال: «الولايات المتحدة وألمانيا تقشان في الاتفاق بشأن التجسس».

New York Times,

<http://www.nytimes.com/2014/05/02/world/europe/us-and-germany-fail-to-reach-a-deal-on-spying>

مارك لاندر (2 أيار 2014). صحيفة نيويورك تايمس. مقال: «ميركل تشير إلى استمرار التوتر مع أميركا بشأن التجسس».

New York Times,

<http://www.nytimes.com/2014/05/03/world/europe/merkelsays-gaps-with-us-over-surveillance-remain.html>.

أندي مولر- ماغوهن وآخرون (14 سبتمبر 2014). صحيفة دير شبيغيل. «خريطة الكنز: انتهاك وكالة الأمن القومي» لـ شركة تكوم، وغيرها من الشركات الألمانية.

Der Spiegel,

<http://www.spiegel.de/international/world/snowden-documents-indicatens-a-has-breached-deutsche-telekom-a-991503.html>

146. يعتقد كثيرون بأن الولايات المتحدة والمملكة المتحدة تتجسّسان كلٌّ على مواطني الأخرى، بهدف الالتفاف على قوانين البلدين. ويكون ذلك شرعياً بمقدار ما تقدران على إقناع نفسيهما بأن «لا مفر منها».

147. جوستان إليوت ونيودريك ميار (11 سبتمبر 2013). موقع «بروبابليكا». مقال: «مزاعم بأن وكالة الأمن القومي» أحبطت مخططاً «ينتشر على الرغم من غياب الأدلة».

Pro Publica,

<http://www.propublica.org/article/claim-on-attacks-thwarted-by-nsa-spreads-despite-lack-of-evidence>.

148. غلين غرينوالد، لورا بواتراس وإيون ماكأسكل (11 سبتمبر 2013). صحيفة الغارديان. مقال: «وكالة الأمن القومي» تشارك إسرائيل معلومات استخباراتية خاما، ضمنها بيانات عن أميركيين».

Guardian,

<http://www.theguardian.com/world/2013/sep/11/nsa-americans-personal-data-israel-documents>.

149. لا تزال الاعتبارات السياسية مهمة. تملك الصين مشكلة كبيرة مع إرهابيي الدايفور، وسترغب بأن تساعد أميركا في التعامل مع ذلك التهديد. وبالطبع، تمتنع أميركا عن مساعدتها؛ لأن إرهاب الدايفور يساهم في إضعاف الصين. شيان- بينغ شونغ (2002). مجلة فورين أفيرز. مقال: «حرب الصين على الإرهاب: 11 سبتمبر والانفصاليون الدايفور».

Foreign Affairs,

<http://www.foreignaffairs.com/articles/58030/chien-peng-chung/chinas-war-on-terror-september-11-and-uighur-separatism>

إليزابيث فان ووي ديفيس (يناير 2008). «مركز دراسات الأمن لمنطقة آسيا- المحيط الهادئ». بحث: «إثنية الدايفور المسلمة الانفصالية في «زينجيانغ»، الصين».

<http://www.apcss.org/college/publications/uyghur-muslim-ethnic-separatism-in-xinjiang-china>

150. جون لافلان (8 سبتمبر 2004). صحيفة الغارديان. مقال: «الشيشان أصدقاء أميركا».

Guardian,

<http://www.theguardian.com/world/2004/sep/08/usa.russia>

سيمون شوستر (19 سبتمبر 2011). مجلة تايم. «كيف استقادت روسيا من الحرب على الإرهاب».

Guardian,

<http://www.theguardian.com/world/2004/sep/08/usa.russia>

جيمس جوردن ميك (19 فبراير 2014). شبكة «إيه بي سي نيوز». مقال: «المعارك السريّة بين القوات الأميركية وإرهابيي الشيشان».

«The secret battles between US forces and Chechen terrorists», *ABC News,*

<http://abcnews.go.com/Blotter/secret-battles-usforces-chechen-terrorists/story?id=22580688>

151. توم وينتر (25 مارس 2014). شبكة «آن بي سي نيوز». مقال: «روسيا حذرت أميركا من تسارنايف، لكنه أفلت بسبب أخطاء في التهجئة».

NBC News,

<http://www.nbcnews.com/storyline/boston-bombing-anniversary/russia-warned-u-s-about-tsarnaevspelling-issue-let-him-n60836>

152. لورا سميث- سبارت ونيك باتون والش (4 فبراير 2014). شبكة «سي آن أن». مقال: «أميركا تكشف «تهديدات محدّدة» لدورة سوتشي الأولمبية».

CNN,

<http://www.cnn.com/2014/02/04/world/europe/russia-sochi-winter-olympics>

الفصل 6 : تعزيز السيطرة المؤسسية

1. وصف أستاذ الاتصالات البروفسور روبرت م. ماكشيسني ذلك التحالف بأنه علاقة اعتماد متبادل بين الحكومات الضخمة والبيانات الضخمة؛ لأنه «زواج عقد في السماء، مع إملات مريرة على الحرية والديمقراطية». روبرت م. ماكشيسني (2013). كتاب: الانفصال الرقمي: كيف تستخدم الرأسمالية الإنترنت ضد الديمقراطية. دار «نيو برس».

http://books.google.com/books/?id=j_7EkTI8kVQC

كنا نعرف عن ذلك حتى قبل سنودن، بفضل مارك كلاين، وهو أحد مطلقي صافرة الإنذار ضد «وكالة الأمن القومي». مارك كلاين (8 يونيو 2006). «إعلان مارك كلاين».

Hepting, et al., v. AT&T, et al., United States District Court, Northern District of California (No. C-06-0672-VRW),

<https://www.eff.org/files/efile/att/Mark%20Klein%20Unredacted%20Decl-Including%20Exhibits.pdf>

أكين ناكاشيما (7 نوفمبر 2007). صحيفة واشنطن بوست. مقال: «قصة رقابة».

Washington Post,

<http://www.washingtonpost.com/wp-dyn/content/article/2007/11/07/AR2007110700006.html>

جيمس بول، لوك هاردينغ وجوليات غارسايد (2 أغسطس 2013). صحيفة الغارديان. مقال: «شركتا «بي تي» و«فودافون» بين شركات اتصالات تقدّم تفاصيل إلى «القيادة الحكومية للاتصالات»».

<http://www.theguardian.com/business/2013/aug/02/telecoms-bt-vodafonecables-gchq>.

4. «فودافون» (2014). وثيقة: «تقرير عن كشف المعلومات إلى قوى إنفاذ القانون».

report, http://www.vodafone.com/content/sustainabilityreport/2014/index/operating_responsibly/privacy_and_security/law_enforcement.html

جوليات غارسايد (5 يونيو 2014). صحيفة الغارديان. مقال: ««فودافون» تكشف وجود خطوط سرّية تتيح رقابة الحكومة».

Guardian,

<http://www.theguardian.com/business/2014/jun/06/vodafone-reveals-secretwires-allowing-state-surveillance>

5. جاك فلورو وغلين غرينوالد (25 أكتوبر 2013). صحيفة لو موند. مقال: «فرنسا في مقعد مشترك مع وكالة الأمن القومي»: استهداف «وانادو» و«ألكاتيل»».

Le Monde,

http://www.lemonde.fr/technologies/article/2013/10/21/france-in-the-nsa-s-crosshair-wanadoo-and-alcatel-targeted_3499739_651865.html

جاك فلورو (21 مارس 2014)، صحيفة لو موند، مقال: «تجسس: كيف تعاونت شركة «أورانج» مع الاستخبارات السرية».

Le Monde,

http://www.lemonde.fr/international/article/2014/03/20/dgse-orange-des-liaison-sincestueuses_4386264_3210.html

6. هيئة الإنذاعة البريطانية (8 إبريل 2014). «بي بي سي نيوز». «المحكمة العليا في «الاتحاد الأوروبي» ترفض قانون الاحتفاظ بالبيانات في دول «الاتحاد الأوروبي»».

BBC News,

<http://www.bbc.com/news/world-europe-26935096>.

7. برنامج الإعلام في إيران (8 أبريل 2013). «الإعلام الرقمي: سلطات الاتصالات تراقب مقامي الإنترنت بواسطة 20 قانوناً جديداً».

Annenberg School for Communication,

<http://www.iranmediaresearch.org/en/blog/218/13/04/08/1322>

8. «مراسلون بلا حدود» (2013). فصل عن فيتنام في كتاب أعدام الإنترنت. <http://surveillance.rsf.org/en/vietnam>

9. راما لاششمي (1 أغسطس 2011). صحيفة واشنطن بوست. مقال: «انتقاد قوانين الهند الجديدة عن الإنترنت».

Washington Post,

http://www.washingtonpost.com/world/indias-new-internet-rules-criticized/2011/07/27/gIQA1zS2mI_story.html.

10. كريس غاي هوناغ (1 أغسطس 2003). مقال: «المساعدون الصغار لـالأخ الكبير»: كيف تعمل شركة «تشويس بوينت» وغيرها من سماسرة المعلومات، على جمع بياناتك وتجهيزها لمصلحة قوى إنفاذ القانون».

North Carolina Journal of International Law and Commercial Regulations 29, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=582302.

جون د. ميكائيلز (6 أكتوبر 2008). مقال: «كل جواسيس الرئيس: شراكات بين الاستخبارات الخاصة والعامة في الحرب على الإرهاب».

California Law Review 96,

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1279867.

11. ماثيول. والد (21 فبراير 2004). صحيفة نيويورك تايمس. مقال: «الولايات المتحدة تصف نشر بيانات شركة «جيت بلو» بأنه غير مناسب».

New York Times,

<http://www.nytimes.com/2004/02/21/business/21blue.html>.

12. «سي آر ستاف» (1 مايو 2003). «الحكومة الأميركية تشتري بيانات 65 ناخباً مكسيكياً مسجلاً». مركز «إنفورميشن كليرنغهاوس».

<http://www.informationclearinghouse.info/article3186.htm>.

13. «الشبكة الأميركية لدعم مكافحة الجرائم المالية» (11 مايو 2014). «متطلبات قانون السرية المصرفية: مرجع سريع عن الخدمات المالية».

http://www.fincen.gov/financial_institutions/msb/materials/en/bank_reference.html

14. كينيث لوي (29 يونيو 2008). صحيفة هيرالد ريفيو. «حصلت «إيلينوي» على 64.3 مليون دولار من بيع بيانات رخص السواقة».

Herald-Review,

http://herald-review.com/business/local/illinois-made-million-selling-driver-s-license-information/article_43c51a15-c885-575e-ac5d-0c01cc9acb6b.html

15. جوي غولن (11 يوليو 2010). مقال: «ولاية أوهايو تكسب ملايين الدولارات من بيع بيانات رخص القيادة مرفقة ببياناتك الشخصية». موقع «بلين ديلار».

Plain Dealer,

http://www.cleveland.com/open/index.ssf/2010/07/ohio_collects_millions_selling.html

16. تيم كاشينغ (13 فبراير 2013). موقع «تيك ديرت». مقال: «ولاية تكساس» تبيع المعلومات الشخصية إلى مئات الشركات، والسائقون غير مسموح لهم بالامتناع.

Tech Dirt,

<http://www.techdirt.com/articles/20130212/21285321958/texas-dmv-sells-personal-information-to-hundreds-companies-drivers-not-allowed-to-opt-out.shtml>.

17. جيف فاينزير (12 أكتوبر 2011). مقال: «ولاية فلوريدا تكسب 63 مليون دولار من بيع معلومات عن السائقين».

Local 10,

<http://www.local10.com/news/Florida-Makes-63M-Selling-Drivers-Info/3078462>

18. كيم زيتير (11 ديسمبر 2003). مجلة وايرد. مقال: «معرض للبيع: الناخب الأمريكي».

Wired,

<http://archive.wired.com/politics/security/news/2003/12/61543>

19. رويينا ماكسون (18 إبريل 2014). صحيفة الغارديان. مقال: «الحكومة البريطانية تبيع البيانات المالية لدافعي الضرائب».

Guardian,

<http://www.theguardian.com/politics/2014/apr/18/hmrc-to-sell-taxpayers-data>

20. رانديب راميش (19 يناير 2014). صحيفة الغارديان. مقال: «الخدمات الصحية الوطنية تجعل بيانات المرضى متاحة لشركات الأدوية والضمان».

Guardian,

<http://www.theguardian.com/society/2014/jan/19/nhs-patient-data-available-companies-buy>

21. سُمي ذلك «تبييض المعلومات». كريس غاي هوفناغل (2 سبتمبر 2014). موقع «سلايت». مقال: «المخادعة الإيحائية في الخصوصية البراغمية».

Slate,

http://www.slate.com/articles/technology/future_tense/2014/09/data_use_regulation_the_libertarian_push_behind_a_new_take_on_privacy.single.html.

22. جيوف دونكان (9 يونيو 2012). موقع «ديجيتال تريندز». مقال: «لماذا لا يحمي خيار عدم التتبع إلى خصوصية الأشخاص».

Digital Trends,

<http://www.digitaltrends.com/mobile/why-do-not-track-may-not-protect-anybodys-privacy>

23. البرلمان الأوروبي والمجلس الأوروبي (24 أكتوبر 1995). «توجيه رقم 95/46/« إي سي» من البرلمان الأوروبي والمجلس الأوروبي في 24 أكتوبر 1995 عن حماية الأفراد فيما يخص التعامل مع البيانات الشخصية وحرية حركة تلك البيانات».

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML>

المجلس الأوروبي (أبريل 2014). «كتاب إرشادي عن القانون الأوروبي لحماية البيانات».

http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf

24. زاك ويتاكر (25 أبريل 2011). موقع «زد دي نت». مقال: «الملاذ الآمن: لماذا نحتاج بيانات الاتحاد الأوروبي» إلى «أن نُحمي» من القانون الأمريكي».

ZDNet,

<http://www.zdnet.com/blog/igeneration/safe-harbor-why-eu-data-needs-protecting-from-us-law/8801>

25. جاي ستانلي (أغسطس 2004). «الاتحاد الأمريكي للحريات المدنية». مقال: «المُرْكَب الرقابي - الصناعي». American Civil Liberties Union, https://www.aclu.org/sites/default/files/FilesPDFs/surveillance_report.pdf
26. دانا بريست ووليام إم. آرकिन (19 يوليو 2010). صحيفة واشنطن بوست. مقال: «عالم خفي، ينمو ليخرج عن السيطرة». *Washington Post*, <http://projects.washingtonpost.com/top-secret-america/articles/a-hidden-world-growing-beyond-control>
27. روبرت أوهارو جونيور، دانا بريست ومارجواريت سنسر (10 يونيو 2013). صحيفة واشنطن بوست. «تسريبات «وكالة الأمن القومي» تظهر مدى اعتماد المؤسسة الاستخباراتية على متعاقدين خارجيين». *Washington Post*, http://www.washingtonpost.com/business/nsa-leaks-put-focus-on-intelligence-apparatus-reliance-on-outside-contractors/2013/06/10/e940c4ba-d20e-11e2-9f1a-1a7cdee20287_story.html
28. لا يبدو مرجحاً أنه امتلك من أوقات الفراغ ما يكفي كي يبتكر أشياء قابلة للتطبيق مباشرة في وظيفته الجديدة. شاين هاريس (29 يونيو 2014). مجلة فورين بوليسي. مقال: «ملك الفضاء السبراني في «وكالة الأمن القومي»، يصبح شركة». *Foreign Policy*, http://www.foreignpolicy.com/articles/2014/07/29/the_crypto_king_of_the_NSA_goes_corporate_keith_alexander_patents
- كونور فيدرسدورف (31 يوليو 2014). مجلة أتلانتيك. مقال: «خطة كيث ألكسندر للغنى السريع ليست أخلاقية». *Atlantic*, <http://www.theatlantic.com/politics/archive/2014/07/keith-alexanders-unethical-get-rich-quick-plan/375367>
29. سينسر إكرمان (17 أكتوبر 2014). صحيفة الغارديان، مقال: «مسؤول رفيع في «وكالة الأمن القومي» يضيء الطريق أمام شركة أمن خاصة». *Guardian*, <http://www.theguardian.com/us-news/2014/oct/17/senior-nsa-official-moonlighting-private-cybersecurity-firm>
30. «إيلمان - غاما غروب» (2011). موقع «ويكيليكس». «الحلول الأمنية الألمانية». *Wikileaks*, <https://s3.amazonaws.com/s3.documentcloud.org/documents/810435/313-elaman-product-list-finisher.pdf>
31. مورغان ماركيز - بوار وبيل ماركز (29 أغسطس 2012). جامعة تورنتو، «مختبر المواطن»، «مركز مونك للدراسات الدولية». مقال: «الهاتف الذكي الذي أحبني: «فن» فيشر» ينتقل إلى الخلوي» <http://citizenlab.org/2012/08/the-smartphone-who-loved-me-finisher-goes-mobile>
- نيكول بيلروث (30 أغسطس 2012). صحيفة نيويورك تايمس. مقال: «برنامج كومبيوتر صمّم ليكشف الجريمة لكنه يستعمل للتجسس على المنشقين». *New York Times*, <http://www.nytimes.com/2012/08/31/technology/finspy-software-is-tracking-political-dissidents.html>

32. بيل ماركزاك وآخرون (17 فبراير 2014). مقال: «رسم تخطيطي لبرنامج كمبيوتر للتجسس من صنع «هاكينغ تيم». جامعة تورنتو، «مختبر المواطن»، «مركز مونك للدراسات الدولية».

<https://citizenlab.org/2014/02/mapping-hacking-teams-untraceablespyware>.

33. فرنون سيلفر وين إلغين (22 أغسطس 2011). شبكة «بلومبرغ نيوز». «التعذيب في البحرين يغدو روتينياً بمساعدة من «نوكيا» و«سيمنز»».

Bloomberg News,

<http://www.bloomberg.com/news/2011-08-22/torture-in-bahrain-becomes-routine-with-help-from-nokia-siemens-networking.html>.

34. مس سميث (10 نوفمبر 2011). مجلة «توروك وورلد». مقال: «مؤتمر التجسس السري للحكومات: كنْ شبحياً، واضرب مئات آلاف الأهداف».

Network World,

<http://www.networkworld.com/article/2221080/microsoft-subnet/secret-snoop-conference-for-gov-t-spying---go-stealth-hit-a-hundred-thousand-target.html>

جنيفر فالنتينو-ديفرز، جوليا أنغوين وستيف ستكلو (19 نوفمبر 2011). صحيفة «ول ستريت جورنال». مقال: «كنز من الوثائق يكشف طرق الرقابة».

Wall Street Journal,

<http://online.wsj.com/news/articles/SB10001424052970203611404577044192607407780>.

Vernon Silver (21 Dec 2011), «Spies fail to escape spyware in \$5 billion bazaar for cyber arms», *Bloomberg News*,

<http://www.bloomberg.com/news/2011-12-22/spies-fail-to-escape-spyware-in-5-billion-bazaarfor-cyber-arms.html>.

35. تدريب في «عالم أي إس إس». (4-3 مارس 2014). دبي، الإمارات العربية.

http://www.issworldtraining.com/iss_mea/Brochure01.pdf

36. تملك «منظمة الشفافية الدولية» لائحة عن حضروا تلك المؤتمرات بين عامي 2006 و2009.

Privacy International (2012), «Surveillance Who's Who»,

<https://www.privacyinternational.org/sww>

37. يووي بيوز ومارسيل روزنباخ (8 ديسمبر 2011). صحيفة «دير شبيغل». مقال: «عدو دولة الشفافية: تكنولوجيا الرقابة الغربية في أيدي الطغاة».

Der Spiegel,

<http://www.spiegel.de/international/world/the-transparent-state-enemy-western-surveillance-technology-in-the-hands-of-despots-a-802317.html>.

38. «فيجنغايين» (8 يناير 2013). وكالة «رويترز» للأنباء. «وفق تقرير «فيجنغايين»، قيمة سوق السلاح السبراني عالمياً 16.9 بليون دولار في العام 2013».

Reuters,

<http://www.reuters.com/article/2013/01/08/idUSNPre7f3zna+100+PRN20130108>

جيمس بامفورد (12 يونيو 2013). مجلة «وايرد». مقال: «الحرب السرية».

Wired,

<http://www.wired.com/2013/06/general-keith-alexander-cyberwar/all>.

39. بول صون ومارغريت كوكر (30 أغسطس 2011). صحيفة «ول ستريت جورنال». مقال: «شركات ساعدت جواسيس ليبين».

Wall Street Journal,

<http://online.wsj.com/news/articles/SB10001424053111904199404576538721260166388>

40. «البابت سيستمز» (24 أبريل 2013). «نالت شركة «البابت سيستمز» عقداً بـ40 مليون دولار كي تمدّ دولة في أفريقيا بنظام «وايز انتليجانز تكنولوجيز»».

- http://ir.elbitsystems.com/phoenix.shtml?c=61849&p=irolnewsArticle&ID=1810121.
41. صحيفة دير شبيغيل (11 أبريل 2012). مقال: «تعمّق المعارضة: مزاعم بيع «سيمنز» نظاماً تقنياً للتعمّق إلى سوريا».
- Der Spiegel*,
http://www.spiegel.de/international/business/ard-reports-siemens-sold-surveillance-technology-to-syria-a-826860.html.
42. بن إلغن وماريون سيلفر (3 نوفمبر 2011). شبكة «بلومبرغ نيوز». مقال: «القمع السوري يلقي معونة من شركة إيطالية وأداة أوروبية-أمريكية للتجسس».
- Bloomberg News*,
http://www.bloomberg.com/news/2011-11-03/syria-crackdown-gets-italy-firm-s-aid-withu-s-europe-spy-gear.html.
43. بول صون ومارغريت كوك (30 أغسطس 2011). صحيفة وول ستريت جورنال. مقال: «شركات ساعدت جواسيس لیبیین».
- Wall Street Journal*,
http://online.wsj.com/news/articles/SB10001424053111904199404576538721260166388
44. سارة كينزيور وكاتي بيرس (11 مايو 2012). موقع «سلايت». مقال: «كيف شيطنت الحكومة الأذربيجانية الإنترنت كي يتتبع المواطنون عنها».
- Slate*,
http://www.slate.com/blogs/future_tense/2012/05/11/azerbaijan_eurovision_song_contest_and_keeping_activists_and_citizens_off_the_internet.html.
45. سارة كينزيور (يوليو 2012). «مؤسسة أميركا الجديدة». بحث: «الحرية الرقمية في التعبير عن الرأي في أوزبكستان: نموذج عن الحجب والسيطرة الاجتماعية».
46. «معهد التكنولوجيا المفتوحة». (9 ديسمبر 2013). وثيقة: «التوصل إلى اتفاقية دولية تمنع تصدير تكنولوجيا الرقابة المكثفة». «مؤسسة أميركا الجديدة».
- New America Foundation,
http://oti.newamerica.net/blogposts/2013/international_agreement_reached_controlling_export_of_mass_and_intrusive_surveillance
47. يووي بيوز ومارسيل روزنباخ (8 ديسمبر 2011). صحيفة دير شبيغيل. مقال: «دعو دولة الشفافية: تكنولوجيا الرقابة الغربية في أيدي الطغاة».
- Der Spiegel*,
http://www.spiegel.de/international/world/the-transparent-state-enemy-western-surveillance-technology-in-the-hands-of-despots-a-802317.html.
48. القائمة الكاملة لتلك البلدان هي: أفغانستان، البحرين، بورما، الصين، مصر، الهند، أندونيسيا، العراق، كينيا، كويت، لبنان، ماليزيا، نيجيريا، قطر، روسيا، السعودية، سنغافورة، كوريا الجنوبية، سوريا، تايلاند، تركيا، فنزويلا. إيرين بواترانتو وفريقها (9 نوفمبر 2011). «وراء «بلو كوت»: تحقيقات عن الترشيح التجاري في سوريا وبورما». جامعة تورنتو، «مختبر المواطن»، «مركز مونك للدراسات الدولية».
- https://citizenlab.org/2011/11/behind-blue-coat.
إيرين بواترانتو وفريقها (29 نوفمبر 2011). «وراء «بلو كوت»: متابعة عن بورما». جامعة تورنتو، «مختبر المواطن»، «مركز مونك للدراسات الدولية».
- Citizen Lab, Munk School of Global Affairs, University of Toronto,
https://citizenlab.org/2011/11/behind-blue-coat-an-update-from-burma.
مورغان-ماركيز بوار وآخرون (24 يونيو 2014). جامعة تورنتو، «مختبر المواطن»، «مركز مونك للدراسات الدولية». مقال: «عالم «بلو كوت»: خريطة عالمية لأدوات التتبع والرقابة».
- Citizen Lab, Munk School of Global Affairs, University of Toronto,

<https://citizenlab.org/2013/01/planet-blue-coat-mapping-global-censorship-and-surveillance-tools>.

49. آدم سنفت وآخرون (20 فبراير 2014). جامعة تورنتو، «مختبر المواطن»، «مركز مونك للدراسات الدولية». مقال: «رقابة الإنترنت في دولة فاشلة: برنامج «نتسويبر» في الصومال».

<https://citizenlab.org/2014/02/internet-filtering-failed-state-case-netsweeper-somalia>

علمي نعمان وآخرون. جامعة تورنتو، «مختبر المواطن»، «مركز مونك للدراسات الدولية». مقال: «يا باكستان نحن نراقبك: تحليل عن دور شركة «نتسويبر الكندية في نظام الحجب في باكستان».

Citizen Lab, Munk School of Global Affairs, University of Toronto,

<https://citizenlab.org/2013/06/o-pakistan>

50. مبادرة الشبكة المفتوحة (12 أكتوبر 2005). وثيقة: «رقابة الإنترنت في بورما 2005».

https://opennet.net/sites/opennet.net/files/ONI_Burma_Country_Study.pdf.

«ضوء جديد على ماينمار» (12 أكتوبر 2005). (16 مايو 2004). مقال: «رئيس الوزراء يحضر حفلًا لإدخال «جدار الوقاية من الفيروسات» الذي تصنعه «فورتينت»».

Firewall, «New Light of Myanmar,

http://www.myanmar.gov.mm/NLM-2004/May04/enlm/May16_h1.html

51. بن أرنولدي (10 أكتوبر 2007). صحيفة كريستيان ساينس مونيتور. مقال: «عندما تصل «برمجيات الرقابة» الأميركية إلى القبضات الإيرانية».

Christian Science Monitor,

<http://www.csmonitor.com/2007/1010/p01s01-ussc.html>.

52. مكتب الأمم المتحدة للمكافحة المخدرات والجريمة. (سبتمبر 2012). وثيقة: «استعمال الإنترنت لأهداف إجرامية».

http://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

53. موقع «بلانيت بيوميتركس» (2 مارس 2011). مقال: «التقنيات البيومترية تنتشر في عالم ديزني». <http://www.planetbiometrics.com/article-details/i/504>.

54. الكونغرس الأمريكي (2012). وثيقة: «وزارة الخارجية تعرب عن تقديرها للتحديثات والتعديلات التقنية لقانون 2012». القانون العام 283.

<http://www.gpo.gov/fdsys/pkg/PLAW-112publ283/html/PLAW-112publ283.htm>

55. شارلي سافاج (7 مايو 2013). صحيفة نيويورك تايمز. مقال: «الولايات المتحدة تقيم عملية تجديد قوانين التتبع».

New York Times,

<http://www.nytimes.com/2013/05/08/us/politics/obama-may-back-fbi-plan-to-wiretap-web-users.html>.

56. شارلي سافاج (27 سبتمبر 2010). صحيفة نيويورك تايمز. مقال: «الولايات المتحدة تحاول تسهيل التتبع على الإنترنت».

New York Times,

<http://www.nytimes.com/2010/09/27/us/27wiretap.html>

57. تيم روجرز (نوفمبر 2013). «القصة الحقيقية لمؤسس «لافابت»».

D Magazine,

<http://www.dmagazine.com/publications/d-magazine/2013/november/real-story-of-lavabit-founder-ladar-levison>

58. سينسر إكرمان (9 أغسطس 2013). صحيفة الغارديان. مقال: «إغلاق مفاجئ لخدمة «لافابت» للبريد الإلكتروني، مع الإشارة إلى تدخل حكومي».

Guardian,

<http://www.theguardian.com/technology/2013/aug/08/lavabit-e-mail-shut-downedward-snowden>

لادار ليفيزون (20 مايو 2014). صحيفة الغارديان. مقال: «أسرار وأكاذيب ويريد سنودن الإلكتروني: لماذا اضطرت إلى إغلاق «لافابت»».

Guardian,

<http://www.theguardian.com/commentisfree/2014/may/20/why-did-lavabit-shut-down-snowden-email>

59. ديكلان ماكولاغ (24 يوليو 2013). موقع «سي نت». مقال: «الشرطة الفيدرالية تضغط على شركات الدوبي» بهدف الحصول على المفاتيح الأساسية للتشفير».

CNET,

<http://www.cnet.com/news/feds-put-heat-on-web-firms-for-master-encryption-keys>

60. ليفيزون مُدّد بالاعتقال لأنه أغلق «لافابت» بأكثر من مسألة السماح للداف بي أي، بالنفاذ غير المشروط لحسابات مستخدميهما كافة. مايكل إزيكوف (13 أغسطس 2013). شبكة «آن بي سي نيوز». مقال: «مالك شركة «لافابت.كوم»: من الممكن اعتقالي بسبب مقاومة أمر بالرقابة».

NBC News,

<http://www.nbcnews.com/news/other/lavabit-com-owner-i-could-be-arrested-resisting-surveillance-order-f6C10908072>.

61. سيرج مالنكوفيتش (21 مارس 2013). نشرة كاسبارسكي دايلي. مقال: «هل يراقب «الأخ الكبير» حسابك على «سكايب»؟»

Kaspersky Lab Daily,

<http://blog.kaspersky.com/skype-government-surveillance>.

جيمس ريزن ونك وينغفيل (20 يونيو 2013). صحيفة نيويورك تايمس. مقال: «وكالة تجسس و«وادي السيليكون» تربطهما تقوية الإنترنت».

New York Times,

<http://www.nytimes.com/2013/06/20/technology/silicon-valley-and-spy-agency-boundby-strengthening-web.html>.

62. شركة «مايكروسوفت». (13 أكتوبر 2011). «مركز أخبار مايكروسوفت». مقال: «مايكروسوفت» تضم «سكايب» رسمياً».

Microsoft News Center,

<http://www.microsoft.com/en-us/news/press/2011/oct11/10-13skypepr.aspx>

63. غلين غرينوالد (11 يوليو 2013). صحيفة الغارديان. مقال: «مايكروسوفت سلّمت «وكالة الأمن القومي» منفذاً إلى الرسائل المشفرة».

Guardian,

<http://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data>

64. كريغ تيمبرغ (11 سبتمبر 2013). صحيفة واشنطن بوست. مقال: «الحكومة الأميركية هدّدت بفرض غرامات ضخمة ما لم يعطها «ياهو» بياناته».

Washington Post,

http://www.washingtonpost.com/business/technology/us-threatened-massive-fine-toforce-yahoo-to-release-data/2014/09/11/38a7f69e-39e8-11e4-9c9f-ebb47272e40e_story.html.

65. جوزيف منن (20 ديسمبر 2013). وكالة «رويترز» للأنباء. مقال: «عقد سري ربط «وكالة الأمن القومي» مع إحدى الشركات الرائدة في صناعة المعلوماتية».

Reuters,

<http://www.reuters.com/article/2013/12/20/us-usa-security-rsa-idUSBRE9BJ1C220131220>

66. المستوى 3 في الاتصالات يحمل الاسم الشيفري «لبلل». وبوجه عام، إذا كان مقدم خدمة الإنترنت الذي تعتمد عليه لديه اسم شيفري في الوكالة، فالأرجح أنك مكشوف. نيكول بيلروث (25 نوفمبر 2013). صحيفة نيويورك تايمس.

New York Times,

<http://www.nytimes.com/2013/11/26/technology/a-peephole-for-the-nsa.html>

67. براندون داووني (30 أكتوبر 2013). موقع «غوغل+». «إنها القصة الكبرى في عالم المعلوماتية الآن».

Google Plus,

<https://plus.google.com/+BrandonDowney/posts/SfYy8xbDWGG>

68. رايان غلامار وغلين غرينوالد (12 مارس 2014). موقع «إنترسبت». «خطة» وكالة الأمن القومي، لنشر برمجيات خبيثة في ملايين الحواسيب».

Intercept,

<https://firstlook.org/theintercept/article/2014/03/12/nsa-plans-infect-millions-computers-malware>.

69. شون غلامار (14 مايو 2014). موقع «آرس تكنيكا». مقال: «صور مصنع والترقية» لوكالة الأمن القومي» تظهر زرع مكونات في محوّلات شركة «سيسكو».

<http://arstechnica.com/tech-policy/2014/05/photos-of-an-nsa-upgrade-factory-show-ciscorouter-getting-implant>

سارة سيلبرت (16 مايو 2014). مقال: «وثيقة حديثة من سنودن تظهر أن وكالة الأمن القومي» اعترضت محوّلات «سيسكو» ودست مكونات فيها».

<http://www.engadget.com/2014/05/16/nsa-bugged-cisco-routers>.

جيمس بول وجوليان بورغر وغلين غرينوالد (5 سبتمبر 2013). صحيفة الغارديان. مقال: «كشف أخيراً: تأزر وكالات التجسس الأميركية والبريطانية في هزيمة الخصوصية والأمن على الإنترنت».

Guardian,

<http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security>

نيكول بلروث وجيف لارسون وسكوت شاين (5 سبتمبر 2013). صحيفة نيويورك تايمس. مقال: «تمكّن وكالة الأمن القومي» من الإطاحة بأساسيات حماية الخصوصية على الدويب».

New York Times,

<http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html>

70. برايان كرييس (28 مايو 2014). «باب خلفي» في معذات رصد المكالمات، هو أداة رقابة».

Krebs on Security,

<http://krebsonsecurity.com/2014/05/backdoor-in-call-monitoring-surveillance-gear>

71. بيتر مأس ولورا بواتراس (10 أكتوبر 2014). موقع «إنترسبت». مقال: «سُر كبير: تملك وكالة الأمن القومي» مخزّين يعملون في ألمانيا والصين».

Intercept,

<https://firstlook.org/theintercept/2014/10/10/core-secrets>

72. مارتن براينت (7 مارس 2014). موقع «نكست ويب». مقال: «غوغل» مطمئن «إلى حدّ كبير» أن البيانات باتت الآن بمنأى عن العيون الحكومية المتفحصة، وفق إريك شميدت».

Next Web,

<http://thenextweb.com/google/2014/03/07/google-pretty-sure-protected-government-spying-eric-schmidt-says>

الفصل 7: العدالة والحرية السياسية

1. ديفيد غرين (27 يناير 2014). «مؤسسة الحدود الإلكترونية». مقال: «غوص في قضية الكنيسة التوحيدية ضد «وكالة الأمن القومي»: عن أهمية الحق في إنشاء روابط».
Electronic Frontier Foundation,
<https://www.eff.org/deeplinks/2014/01/deep-divefirst-unitarian-church-v-nsa-why-freedom-association-matters>
2. جوشوا إيتون (15 أغسطس 2014). موقع «يو يو ورلد». مقال: «تحدي دولة الرقابة».
UU World,
<http://www.uuworld.org/ideas/articles/297088.shtml>
3. يوشاي بنكر (13 سبتمبر 2013). صحيفة الغارديان. «حان الوقت للوقوف بوجه التلاعب الوحشي لدوكالة الأمن القومي» بحقوقنا».
Guardian,
<http://www.theguardian.com/commentisfree/2013/sep/13/nsa-behemoth-trampling-rights>.
4. مجلة الإيكونوميست (16 نوفمبر 2013). مقال: «العالم المُسجَّل: كل خطوة تخطوها».
Economist,
<http://www.economist.com/news/leaders/21589862-cameras-become-ubiquitous-and-able-identify-people-more-safeguards-privacy-will-be>
5. هارفي سيلفرغليت وتيم لينش (يناير/فبراير 2010). تقرير «معهد كاتو للسياسة». «تجريم الأشياء كلها تقريباً».
Cato Policy Report,
<http://www.cato.org/policy-report/januaryfebruary-2010/criminalization-almost-everything>.
هارفي سيلفرغليت (2011). كتاب ثلاث جنايات يومياً: عن استهداف ضباط الشرطة للأبرياء. دار «إينكاونتر» للكتب.
<http://www.threefeloniesaday.com>.
G. H. Reynolds (8 Jul 2013), «Ham sandwich nation: Due process when everything is a crime,»
Columbia Law Review 113,
http://columbialawreview.org/ham-sandwich-nation_reynolds
6. روز سيوتا (4 مايو 2003). صحيفة فيلادلفيا إنكوايرر. مقال: «نقاد يرصدون توسعاً في قوانين الدليل المادي».
Inquirer,
http://articles.philly.com/2003-05-04/news/25460033_1_material-witness-law-material-witnesses-material-witness-statute
أنيا مالهوترا (27 يونيو 2005). منظمة «هيومن رايتس ووتش». «شاهد على إساءة الاستخدام: الإساءة إلى حقوق الإنسان في قانون الدليل المادي، منذ 11 سبتمبر».
Anjana Malhotra (27 Jun 2005), «Witness to abuse: Human rights abuses under the Material Witness Law since September 11,» Human Rights Watch,
http://www.hrw.org/sites/default/files/reports/us0605_0.pdf.
Naureen Shah et al.(21 Jul 2014), «Illusion of justice: Human rights abuses in US terrorism prosecutions,» Human Rights Watch,
<http://www.hrw.org/node/126101>
7. في ولاية «كارولينا الشمالية» تعدُّ بندقية الصيد المقصوفة الماسورة سلاحاً للدمار الشامل. جوناثان ليمير (30 أغسطس 2011). صحيفة نيويورك ديلي تايمس. مقال: «إدانة طالب في «كارولينا الشمالية» لأنه تباهى بامتلاك بندقية صيد مقصوفة الماسورة».

<http://www.nydailynews.com/news/national/northcarolina-student-charged-weapon-mass-destruction-toting-sawed-off-shotgunarticle-1.950971>

8. لويس جاكوبسون (9 يوليو 2013). موقع «بوليتي فاكْت». مقال: «ما هو تعريف الإرهاب؟»

Politifact,

<http://www.politifact.com/truth-o-meter/article/2013/jul/09/whats-definition-terrorism>

9. دانيال ج. سولوف (2004). كتاب الإنسان الرقمي: التكنولوجيا والخصوصية في عصر المعلومات. «مطبعة جامعة نيويورك».

<http://docs.law.gwu.edu/facweb/dsolove/Digital-Person/text/Digital-Person-CH3.pdf>

10. اعتادت «وزارة الأمن الوطني» - وربما ما زالت - أن تراقب الشبكات الاجتماعية كي تراقب ردود أفعال الناس على أخبار «مسيئة الولايات المتحدة». إلين ناكاشيما (13 يناير 2012)، صحيفة واشنطن بوست. مقال: «يفشى نشطاء الحريات المدنية من مراقبة «وزارة الأمن الوطني» للشبكات الاجتماعية».

Washington Post,

http://www.washingtonpost.com/world/national-security/dhs-monitoring-of-social-mediaworries-civil-liberties-advocates/2012/01/13/gIQAPO7wP_story.html.

11. هيئة الإذاعة البريطانية (31 يناير 2012). مقال: «يُنصح بتوخي الحذر على «تويتر»، بعد منع سَوَاح من دخول أمريكا».

BBC News,

<http://www.bbc.co.uk/news/technology-16810312>

12. غري سميث (25 يونيو 2014). صحيفة هافنغتون بوست. «كيف يقرأ البوليس «تويتر» كله بحثاً عن مخاطر إرهابية».

Huffington Post,

http://www.huffingtonpost.com/2014/06/25/dataminr-mines-twitter-to_n_5507616.html.

13. فيليب ميسنغ (13 أبريل 2013). صحيفة نيويورك بوست. مقال: «اعتقال راكب في مطار «جي أف كيه» لتحذره عن سديوتش «قنبلة»».

New York Post,

<http://nypost.com/2013/04/13/jfk-passenger-detained-after-talking-about-bomb-sandwich>

14. هناك مقال ممتاز عن ذلك الموضوع.

براكسيس (17 يناير 2014). موقع «ميديوم». مقال: «العالم كله أصبح الآن مطاراً: الرقابة والسيطرة الاجتماعية».

Medium,

<https://medium.com/i-m-h-o/9a1e5268ff39>.

15. لورين راسل (24 أبريل 2013). شبكة «سي أن أن». مقال: «عندما يؤدي الإفراط في مشاركة المحتوى على الإنترنت إلى اعتقالك».

CNN,

<http://www.cnn.com/2013/04/18/tech/social-media/online-oversharing-arrests>

16. «هيئة الإذاعة البريطانية» (27 مارس 2012). مقال: «فابريس موامبا: مغرّد عنصري على «تويتر»، يسجن 56 يوماً».

BBC News,

<http://www.bbc.co.uk/news/uk-wales-17515992>.

17. «هيئة الإذاعة البريطانية» (4 يونيو 2014). مقال: «رجل يسجن بسبب تدوينه على «فيسبوك» عدت مسيئة لأن ماغواير».

BBC News,

<http://www.bbc.co.uk/news/uk-england-27696446>

18. جبرمي سكاميل وتغلين غرينوالد (10 فبراير 2014). موقع «إنترسيت». مقال: «الدور السري لـ«وكالة الأمن القومي» في برنامج الاغتيال الأمريكي».

Intercept,

<https://firstlook.org/theintercept/article/2014/02/10/the-nsas-secret-role>

كوري كريد (4 مارس 2014). قناة «الجزيرة» التلفزيونية. مقال: «القتل باسم الخوارزميات».

Al Jazeera,

<http://america.aljazeera.com/opinions/2014/3/drones-big-data-waronterrorobama.html>

19. جون كاغ وسارة كريبيس (2014). كتاب: أسلحة حرب الـ«درون». دار «ويلي» للنشر.

<http://books.google.com/books?id=ISoOBAAAQBAJ>.

20. ريتشارد إنغل وروبرت ويندريم (5 يونيو 2013). شبكة «أن بي سي نيوز». مقال: «وثائق تظهر أن السدي أي إيه» لم تكن تعرف نصف من قتلهم بغارات الـ«درون».

NBC News,

http://investigations.nbcnews.com/_news/2013/06/05/18781930-ciadidnt-always-know-who-it-was-killing-in-drone-strikes-classified-documents-show.

21. كارين ماكفيل (27 أغسطس 2013). صحيفة «الغارديان». مقال: «وفق «الاتحاد الأمريكي للحريات المدنية»، يخالف برنامج رقابة الدوكالة الأمن القومي» الدستور».

Guardian,

<http://www.theguardian.com/world/2013/aug/27/nsa-surveillance-program-illegal-actu-lawsuit>

22. أوليفر أوغست (23 أكتوبر 2007). مجلة «ايرد». «جدار النار العظيم»: محاولة الصين المتخبطة والمبينة للسيطرة على ما يحدث على الدويب».

Wired,

http://www.oliveraugust.com/journalism_chinas-internet-heroes.htm.

23. غاري كينغ وجنيفر بان ومارغريت ي. روبرتس. (مايو 2013). مجلة «أميركان بوليتيكال ساينس ريفيو». مقال: «كيف يعمل الحجب في الصين على إثارة الانتقاد ضد الحكومة، لكنه يخرس حرية التعبير الجماعية».

American Political Science Review 107,

<http://gking.harvard.edu/publications/how-censorship-china-allows-government-criticism-silences-collectiveexpression>

24. سايتن ديوي (12 أغسطس 2013). صحيفة «واشنطن بوست». مقال: «تقف «ويكيبيديا» شبه وحيدة في مواجهة طلبات صينية بممارسة رقابة ذاتية».

Washington Post,

<http://www.washingtonpost.com/blogs/worldviews/wp/2013/08/12/wikipedia-largely-alone-in-defying-chinese-self-censorship-demands>

25. رونالد دايرت وآخرون (2010). كتاب: «النفاذ تحت السيطرة: رسم شكل السلطة والحقوق والدور في القضاء السبراني» (مطبعة «معهد ماساشوستس للتقنية»).

MIT Press,

<http://mitpress.mit.edu/books/access-controlled>.

26. مجلة «فورييس». (25 ديسمبر 2000). مقال: «سوازتيكا. كوم».

Forbes,

<http://www.forbes.com/forbes/2000/1225/6616164s1.html>

27. «هيئة الإنذاعة البريطانية» (1 سبتمبر 2013). مقال: «تفعيل القيود على الإنترنت في فيتنام».

BBC News,

<http://www.bbc.com/news/world-asia-23920541>.

28. رونالد دايرت وآخرون (2010). كتاب: «النفاذ تحت السيطرة: رسم شكل السلطة والحقوق والدور في القضاء السبراني» (مطبعة «معهد ماساشوستس للتقنية»).

MIT Press,

<http://mitpress.mit.edu/books/access-controlled>

29. بن كوين (10 أكتوبر 2011). صحيفة الغارديان. مقال: «الشركات الأربع الأربعة الكبرى لتقديم خدمة الإنترنت في بريطانيا، تنتقل إلى «خيار عدم الخروج من الرقابة» بالنسبة للجنس الإباحي».

Guardian,

<http://www.theguardian.com/society/2011/oct/11/pornography-internet-service-providers>

أنطوني فيولا (28 سبتمبر 2013). صحيفة واشنطن بوست. مقال: «الإجراءات البريطانية الصارمة في الرقابة شبكياً لمواد الجنس الإباحي، تثير نقاشات عن حرية التعبير».

Washington Post,

http://www.washingtonpost.com/world/europe/britainsharsh-crackdown-on-internet-porn-prompts-free-speech-debate/2013/09/28/d1f5caf8-2781-11e3-9372-92606241ae9c_story.html.

30. إيوين ماكأسكل (1 ديسمبر 2010). صحيفة الغارديان. مقال: «ضغط سياسي يؤدي إلى سحب موقع «ويكيليكس» من «أمازون. كوم»».

Guardian,

<http://www.theguardian.com/media/2010/dec/01/wikileaks-website-cables-servers-amazon>.

31. نيل ماكفاركوهار (6 مايو 2014). صحيفة نيويورك تايمس. مقال: «بهودو»، روسيا تشدد قوانين الإنترنت بفرضها «قانون البلوغرز».

New York Times,

<http://www.nytimes.com/2014/05/07/world/europe/russia-quietly-tightens-reins-on-web-with-bloggers-law.html>

32. يؤدي جعل المواطن مخبراً إلى تسميم المجتمع. إذ يخلق رعباً واسعاً يوصل إلى تفكيك الأوصار الاجتماعية التي تربط الناس بعضها بعضاً. بروس شنابير (26 أبريل 2007). مدونة إلكترونية. مقال: «في التمييز بين المخبر «الكريه» والمخبر للمواطن».

Schneier on Security,

https://www.schneier.com/blog/archives/2007/04/recognizing_hin_1.html

33. جاسون كيو إنغ (12 مارس 2012). موقع «وايبنغ نون فايولانس». مقال: «كيف جعلت الصين الإنترنت تراقب نفسها بنفسها؟»

Waging Nonviolence,

<http://wagingnonviolence.org/feature/how-china-gets-the-internet-to-censor-itself>

34. كوينغ بانغ (2008). مجلة دراسات الاتصال العالمي. دراسة: «الحجب الذاتي وصعود الجماعة على الإنترنت: دراسة أنثروبولوجية لمجتمع الصين الافتراضي».

<http://www.uri.edu/iaics/content/2008v17n3/05%20Cuiming%20Pang.pdf>.

35. جورج ل. وايت وفيليب ج. زيمباردو (مايو 1975). «مكتب البحرية الأمريكية للبحوث». دراسة: «التأثيرات المجددة للرقابة: نزاع الفردية والتفاعل».

Office of Naval Research/National Technical Information Service,

<http://www.dtic.mil/dtic/tr/fulltext/u2/a013230.pdf>.

36. «الحكمة العليا الأمريكية» (23 يناير 2012). قرار عن «الولايات المتحدة ضد جونز».

<http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=US&navby=case&vol=000&invol=10-1259#opinion1>.

37. إيبين موغلين (27 مايو 2014). صحيفة الغارديان. مقال: «الخصوصية تتعرض للهجوم: وثائق وكالة الأمن القومي» تكشف تهديدات جديدة للديمقراطية».

Guardian,

<http://www.theguardian.com/technology/2014/may/27/-sp-privacy-under-attack-nsa-files-revealed-new-threats-democracy>.

38. ج. أليكس سنها (28 يوليو 2014). مؤسسة هيومن رايتس ووتش. مقال: «لديهم حرية أن يراقبوا الجميع». Human Rights Watch,

<http://www.hrw.org/reports/2014/07/28/libertymonitor-all>.

39. في العام 2014، علمنا أن المديرية الأسترالية للإشارات، وهي الصنو الأسترالي لدوكالة الأمن القومي، تنصت على الاتصالات بين شركة «ماير براون» الأميركية للاستشارات القانونية وزيوتها الممثلة في الحكومة الأندونيسية. وأعطت المديرية الأسترالية تلك البيانات إلى الوكالة. جيمس رايزن ولورا بواتراس (15 فبراير 2014). صحيفة نيويورك تايمس. مقال: «تجسس شريك لدوكالة الأمن القومي» شمل شركة أمريكية للاستشارات القانونية.

New York Times,

<http://www.nytimes.com/2014/02/16/us/eavesdropping-ensnared-american-law-firm.html>

40. ج. أليكس سنها (28 يوليو 2014). مؤسسة هيومن رايتس ووتش. مقال: «لديهم حرية أن يراقبوا الجميع». Human Rights Watch,

<http://www.hrw.org/reports/2014/07/28/libertymonitor-all>.

41. رابطة «بين أمريكا» (2013). «تأثيرات مزعومة: رقابة وكالة الأمن القومي» تدفع الكتاب إلى الحجب الذاتي». http://www.pew.org/sites/default/files/Chilling%20Effects_PEN%20American.pdf.

42. جرى الاستطلاع مباشرة عقب ظهور الأخبار الأولى عن جمع «وكالة الأمن القومي» للدميتات، من شركة «فريزون»، وافترضاً من كل شخص آخر؛ وحصولها على بيانات الإنترنت من شركات كدغول، و«ياهو»، و«فيسبوك»، و«مايكروسوفت»، و«تويتر». إليزابيث دويسكن (26 أغسطس 2014). صحيفة وول ستريت جورنال. مقال: «استطلاع: الناس لا يتحدثون عن وكالة الأمن القومي» على الإنترنت.

Wall Street Journal,

<http://blogs.wsj.com/digits/2014/08/26/survey-people-dont-want-to-talk-online-about-the-nsa>

43. أرميتا جايكومار (2 أبريل 2014). صحيفة واشنطن بوست. مقال: «أمريكيون يقولون إنهم صاروا يتسوقون أقل على الإنترنت. الملامة تقع على وكالة الأمن القومي».

Washington Post,

<http://www.washingtonpost.com/blogs/the-switch/wp/2014/04/02/americans-say-theyre-shopping-less-online-blame-the-nsa>

44. داويندر س. سيدهو (2007). «التأثير المفزع لرقابة الحكومة في استخدام الإنترنت من قبل المسلمين الأمريكيين».

University of Maryland Law Journal of Race, Religion, Gender and Class 7,

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1002145

45. ديفيد غرين (6 نوفمبر 2013). «مؤسسة الحقوق الإلكترونية». مقال: «ملفات مؤسسة الحقوق الإلكترونية»: 22 شهادة مباشرة عن الفزع الذي أثارته رقابة «وكالة الأمن القومي»، بشأن الحق في الترابط.

<https://www.eff.org/press/releases/eff-files-22-firsthand-accounts-hownsa-surveillance-chilled-right-association>

46. أليكس مارشوز وكاثارين توكر (24 مارس 2014). «شبكة بحوث علم الاجتماع». ورقة بحث: «الرقابة الحكومية وسلوك البحث على الإنترنت».

Social Science Research Network,

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2412564

47. «المفوضية العليا لحقوق الإنسان في الأمم المتحدة» (30 يونيو 2014). «العصر الرقمي والحق في الخصوصية». http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf.

48. ليز كلايمز (22 مارس 2012). موقع «بلايز». مقال: «مجرد زيارة موقع شبكي لإرهابيين تؤدي إلى السجن في فرنسا».

Blaze,

<http://www.theblaze.com/stories/2012/03/22/simply-visiting-terrorist-websites-could-mean-jail-time-infrance>.

49. راشيل كلارك (11 يوليو 2013). مقال: «كل شيء عن كل شخص: عمق رقابة الدستور في جمهورية ألمانيا الديمقراطية».

<http://thevieweast.wordpress.com/2013/07/11/everything-about-everyone-the-depth-of-stasi-surveillance-inthe-gdr>.

أوكا إيفاجين (20 أغسطس 2014). مقال: «مكالماتكم الهاتفية ستراقب قريباً».

<http://pulse.ng/lifestyle/tech/security-vs-privacy-your-calls-may-soon-be-monitored-ncc-id3066105.html>.

50. كارل غواشيم فريدرتش (أكتوبر 1939). «الديمقراطية والتمرد».

Political Quarterly 10,

<http://onlinelibrary.wiley.com/doi/10.1111/j.1467-923X.1939.tb00987.x/abstract>.

51. بروس شناير (2012). كتاب: كَذِبَة ومتمردون: تفعيل الثقة التي يحتاجها المجتمع لينمو. دار «ويلي» للنشر.

<http://www.wiley.com/WileyCDA/WileyTitle/productCd-1118143302.html>.

52. فرانك زايا وبيتر أوشيوكوسو (1989). كتاب: كتاب فرانك زايا الحقيقي. دار «بوزيدون برس».

http://books.google.com/books?id=FB00_HCpBy0C.

53. يشد أستاذ القانون في «جامعة واشنطن» البروفسور نيل ريتشاردز على تلك الفكرة بالقول: «تتطور الأفكار الجديدة بأفضل الطرق، عندما تكون بعيدة عن التدقيق المتخصص للكشف العمومي». نيل ريتشاردز (مايو 2013) بحث: «مخاطر الرقابة».

Harvard Law Review 126,

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2239412

54. تستخدم السلطات المحلية في مدينة «بلتيمور» الصور الجوية في ملاحظة مخالفات البناء، إذ تراقبها مع قاعدة بياناتها عن رخص البناء. دوو دونوفان (7 سبتمبر 2004). صحيفة «بلتيمور صن». مقال: «نظرة من فوق لكل مبنى في المدينة».

Baltimore Sun,

http://articles.baltimoresun.com/2004-09-07/news/0409070310_1_images-deck-aerial

55. غريغوري كونتي (4 أبريل 2014). «نظرية للبقاء بالنسبة للحكومة والإنفاذ المؤتمت للقانون».

http://robots.law.miami.edu/2014/wp-content/uploads/2013/06/Shay-et-al-TheoryofConservation_final.pdf.

56. يصلح نموذجاً على ذلك «الشرطي أكل لحوم البشر» الذي درش في الإنترنت مع أصدقائه، عن اغتصاب زوجته والتهامها مع أخريات؛ لكنه لم يفعل شيئاً. دانيال بيكرمان وداريه غريغوريان (1 يوليو 2014). صحيفة نيويورك تايمس. مقال: «إطلاق سراح الشرطة أكل لحوم البشر»، بعد أن انقلبت أمور التهمة بشكل مذهل.

New York Daily News,

<http://www.nydailynews.com/new-york/nyc-crime/conviction-cannibal-nypd-overtured-article-1.1850334>.

Daniel Engber (2 Jul 2014), «The cannibal cop goes free, but what about the murderous mechanic?».

Slate,

http://www.slate.com/articles/news_and_politics/crime/2014/07/the_cannibal_cop_gilberto_valle_goes_free_what_about_michael_van_hise_and.html.

57. والتر بيرى وآخرون (2013). «مؤسسة راند». بحث: «شرطة توقعية: دور توقع الجرائم في عمليات إنفاذ القانون».
- RAND Corporation,
<https://www.ncjrs.gov/pdffiles1/nij/grants/243830.pdf>.
58. مايكل ل. ريتش (مارس 2013). مجلة هارفرد للقانون والسياسة العامة. بحث: «أجب علينا جعل الجريمة مستحيلة».
- Harvard Journal of Law and Public Policy* 36,
http://www.harvard-jlpp.com/wp-content/uploads/2013/04/36_2_795_Rich.pdf
59. يوشاي بنكر (4 ديسمبر 2013) «مركز بحوث جامعة هارفرد عن الحوسبة والمجتمع». بحث: «النظام والضمير: الرقابة الواسعة لوكالة الأمن القومي، ومسألة الحرية».
- Center for Research on Computation and Society, Harvard University,
<http://crs.seas.harvard.edu/event/yochai-benklercrs-lunch-seminar>
 and
<https://www.youtube.com/watch?v=6EUeRpCzpw>
60. وليام ي. كولبي (1976). مجلة الأمن الدولي. مقال: «الأمن وسرية الاستخبارات في المجتمع الحر».
- International Security* 1,
<http://people.exeter.ac.uk/mm394/Intelligence%20Secrecy%20and%20Security.pdf>
- جيمس ي. نوت (صيف 1975). مقال: «السرية والاستخبارات في مجتمع حر».
- Studies in Intelligence* 19,
https://www.cia.gov/library/centerfor-the-study-of-intelligence/kent-csi/vol19no2/html/v19i2a01p_0001.htm
61. بامبلا و. لونغ وأليكس رولاند (1994). بحث: «السرية العسكرية في الماضي وفي أوروبا القرون الوسطى: تقييم نقدي». مجلة هستوري أند تكنولوجي.
- History and Technology* 11,
<http://www.tandfonline.com/doi/abs/10.1080/07341519408581866?journalCode=ghat20>
62. لويس أ. كوزر (صيف 1963). مقال: «اختلالات وظيفية في السرية العسكرية». مجلة سوشال بروبلمز.
- Social Problems* 11,
<http://www.jstor.org/discover/10.2307/798801>
63. كان المثلث الأبرز على ذلك هو السرية والخداع اللذان أحاطا بعملية إنزال قوات الحلفاء على شواطئ النورماندي، جون س. ويندل (1997). سلاح الجو الأمريكي. تقرير: «عملية الخداع الاستراتيجي التي رافقت غزو النورماندي».
- <http://www.globalsecurity.org/military/library/report/1997/Wendell.htm>
- دان لاموث (6 يونيو 2014). صحيفة واشنطن بوست. مقال: «ذكرى الأكاذيب والسرية العسكرية التي أنجحت الإنزال على النورماندي».
- Washington Post*,
<http://www.washingtonpost.com/news/checkpoint/wp/2014/06/06/remembering-the-military-secrecy-and-liesthat-made-d-day-successful>.
64. سيفن أفترغود (أكتوبر 1999). «مركز جامعة كورنيل لدراسات السلام». ورقة بحث: «السرية الحكومية وإنتاج المعرفة: مسح إحصائي عن بعض القضايا العامة».
- <http://large.stanford.edu/publications/crime/references/dennis/occasional-paper23.pdf>.
- Francis B. Kapper (Oct 1999), «The role of government in the production and control of scientific and technical knowledge», ibid
- كوين فارمر ودانيال ماغوسكي (يونيو 2012). مجلة بريتش جورنال أوف هستوري أوف ساينس. ورقة بحث: «ولايات السرية: مدخل».

British Journal of the History of Science 45,

<http://journals.cambridge.org/action/displayAbstract?fromPage=online&aid=8608487&fileId=S0007087412000052>

65. بيتر غاليسون (خريف 2004)، «كريتيكال إنكوايري»، مقال: «إزالة المعرفة».

Critical Inquiry 31,

<http://www.fas.harvard.edu/~hsdept/bios/docs/Removing%20Knowledge.pdf>.

66. المرجع السابق.

67. «المكتب الأمريكي للإدارة والموازنة» (فبراير 2014). تقرير: «مراجعة العمليات الأمنية ومدى تناسبتها».

<http://www.fas.org/sgp/othergov/omb/suitsec-2014.pdf>.

68. وفق كلايبر، وهو مدير الاستخبارات القومية: «الكشف عن المعلومات تكون سرية وتتصل بالتفاصيل العملية لوكالة الأمن القومي» وأمديتها، وفق ما ورد في تلميحات المدعين: من شأنه أن يتسبب بضرر بالغ للأمن القومي للولايات المتحدة».

جيمس ر. كلايبر (20 ديسمبر 2013). «إعلان عام من جيمس ر. كلايبر، مدير الاستخبارات القومية».

Jewel et al. v. National Security Agency et al. (08-cv-4873-

JSW; Shubert, et al., v. Obama, et al. (07-cv-693-JSW), United States District Court for the Northern District of California,

<http://www.dni.gov/files/documents/1220/DNI%20Clapper%202013%20Jewel%20Shubert%20SSP%20Unclassified%20Signed%20Declaration.pdf>

69. بعد كشوفات سنودن، رفعت محكمة «قيسا» غطاء السرية عن معظم أحكامها العامة. ولم يكن ليحصل ذلك الأمر أيضاً لو لم يفعل سنودن ما فعله.

70. جنيفر فالنتينو-دي فرايز (2 يونيو 2014). صحيفة وول ستريت جورنال. مقال: «ملفات مغلقة لإحدى المحاكم، عن المساعدة في تموية الرقابة الإلكترونية».

Wall Street Journal,

http://online.wsj.com/news/article_email/sealed-court-files-obscurerise-in-electronic-surveillance-1401761770-lMyQjAxMTA0MDAwMzEwNDMyWj

71. جوزيف كوكس (7 أغسطس 2014). موقع «فايس». مقال: «لا تعترف الشرطة البريطانية أنه يتتبع المكالمات الهاتفية للناس».

Vice,

<http://motherboard.vice.com/read/uk-police-wont-admit-theyre-tracking-peoples-phone-calls>

72. ثمة قصة عن المعاشية المباشرة لتجربة تلقي ذلك النوع من رسائل «وكالة الأمن القومي». في البداية، نُشرت تلك القصة باعتبارها من مجهول، ثم تبين أنها لبروستر كاهيل، مؤسس «أرشيف الإنترنت». مجهول (23 مايو 2007). صحيفة واشنطن بوست. مقال: «رسالة إلي من الأمن القومي، مع أمر قضائي بالصمت».

<http://www.washingtonpost.com/wp-dyn/content/article/2007/03/22/AR2007032201882.html>

73. 623 كيم زتر (3 مارس 2014). مجلة وايرد. مقال: «سلاح سري لشرطة فلوريدا: تتبع الهواتف من دون مذكرات قضائية».

Wired,

<http://www.wired.com/2014/03/stingray>

كيم زتر (4 مارس 2014). مجلة وايرد. مقال: «عقدت الشرطة مع صانع محلي لأداة تتبع، يمنع الحديث عن تلك الأداة».

Wired,

<http://www.wired.com/2014/03/harris-stingray-nda>

74. داروين بوند-غراهام وآلي ونستون (30 أكتوبر 2013). مجلة سان فرانسيسكو ويكلي. مقال: «كل جرائم الغد: مستقبل الشرطة يبدو أقرب إلى التصنيف في ماركات تجارية».

SFWeekly,

<http://www.sfweekly.com/2013-10-30/news/predpol-sfpd-predictive-policingcompstat-lapd/full>.

75. جينيفر ك. إلسا (10 يناير 2013). بحث: «حماية المعلومات السرية: الإطار القانوني».

Congressional Research Service,

<http://fas.org/sgp/crs/secretary/RS21900.pdf>.

76. كاري نيوتن ليون (2007). «لويس أند كلارك لو ريفيو». تقرير: «خطوة أسرار الدولة: توسع مداها مع إساءة الحكومة استخدام السلطة».

Lewis and Clark Law Review 99,

<http://www.fas.org/sgp/jud/statesec/lyons>

سودما سيتي (يوليو 2012). مجلة كونكتيكت لو ريفيو. مقال: «صعود أسرار الأمن القومي».

Connecticut Law Review 44,

<http://connecticutlawreview.org/files/2012/09/5.Setty-FINAL.pdf>

77. إريك ليشتبلاو وسكوت شاين (9 يوليو 2006). صحيفة نيويورك تايمس. مقال: «أحد الحلفاء نصح بوش بإبقاء التجسس بعيداً عن الكونغرس».

New York Times,

<http://www.nytimes.com/2006/07/09/washington/09hoekstra.html>

سكوت شاين (11 يوليو 2009). صحيفة نيويورك تايمس. مقال: «صلة شيني بإخفاء مشروع للدي أي إيه».

New York Times,

<http://www.nytimes.com/2009/07/12/us/politics/12intel.html>.

بول لويس (31 يوليو 2013). صحيفة الغارديان. مقال: «البيت الأبيض يعجز عن تأكيد إبلاغه الكونغرس عن برنامج «وكالة الأمن القومي» في التجسس».

Guardian,

<http://www.theguardian.com/world/2013/jul/31/white-house-congress-nsa-xkeyscore>

78. بارتون غيلمان (15 أغسطس 2013). صحيفة واشنطن بوست. مقال: «ما نقول، وما لا نقول؛ لمن «يشرفون» علينا».

Washington Post,

<http://apps.washingtonpost.com/g/page/national/what-to-say-and-not-to-say-to-our-overseers/390>.

79. غلين غرينوالد (4 أغسطس 2013). صحيفة الغارديان. مقال: «أعضاء في الكونغرس يُمنعون من معلومات

أساسية عن «وكالة الأمن القومي»».

Guardian,

<http://www.theguardian.com/commentisfree/2013/aug/04/congress-nsa-denied-access>

80. سينر إيكerman (14 أغسطس 2013). صحيفة الغارديان. مقال: «دَحْ مجتمعات الاستخبارات على شرح سبب التكتّم على وثائق حسّاسة».

Guardian,

<http://www.theguardian.com/world/2013/aug/14/nsa-intelligence-committeeunder-pressure-document>.

81. تشارلي سافاج ولورا بواتراس (11 مارس 2013). صحيفة نيويورك تايمس. مقال: «كيف تطوّرت محكمة سرية، وزادت في قدرة جواسيس أميركا».

New York Times,

<http://www.nytimes.com/2014/03/12/us/how-a-courts-secret-evolution-extendedspies-reach.html>.

82. إميل بيترسون (30 سبتمبر 2011). «لجنة مراسلين من أجل حرية الصحافة». تقرير: «طلي الكتمان: أسرار المحكمة العليا».

Reporters Committee for Freedom of the Press,
http://www.rcfp.org/browse-media-law-resources/news-media-law/news-media-law-summer-2011/under-seal-secrets-supreme-court

83. كورا كورير (30 يوليو 2013). موقع «بروبابليكا». مقال: «سجل الرئيس أوباما في قمع مسري وثائق الأمن القومي».

Pro Publica,
http://www.propublica.org/special/sealing-loose-lips-charting-obamas-crackdown-on-national-security-leaks

84. ليوناردو داووني جونور وسارة رافسكي (أكتوبر 2013). «لجنة حماية الصحفيين». مقال: «التحقيقات في التبريات والرقابة في أميركا ما بعد 9/11».

https://www.cpj.org/reports/2013/10/obama-and-the-press-us-leaks-surveillance-post-911.php.

ديفيد بوزن (20 ديسمبر 2013). مجلة هارفرد لوي ريفيو. مقال: «وحش ليفيانثان المُسرب: كيف تدن الحكومة وتشجع الكشف غير المشروع عن الوثائق».

Harvard Law Review 127,
http://harvardlawreview.org/2013/12/the-leaky-leviathan-why-the-government-condemns-and-condones-unlawful-disclosures-of-information.

85. دانيال إلسبرغ (30 مايو 2014)، صحيفة الغارديان. مقال: «سنودن لن يحظى بمحاكمة عادلة، وكيري على خطأ».

Guardian,
http://www.theguardian.com/commentisfree/2014/may/30/daniel-ellsberg-snowden-fair-trial-kerry-espionage-act.

86. ديفيد ديسهنو (20 يوليو 2012). وكالة أنباء «أسوشيتد برس». مقال: «منع تشيلسا ماننغ من مناقشة أضرار «ويكيليكس»».

Associated Press,
http://seattletimes.com/html/nationworld/2018724246_apusmanningwikileaks.html

87. هناك انقسام أمريكي حول تلك النقطة. سيث موتيل (15 أبريل 2014). مقال: «تغطية «وكالة الأمن القومي» تنال جائزة «بوليتزر»، لكن الأميركيين منقسمون حول تسيريات سنودن».

Pew Research Center,
http://www.pewresearch.org/fact-tank/2014/04/15/nsa-coverage-wins-pulitzer-but-americans-remain-divided-onsnowden-Leaks

88. جوناثان توباز (28 مايو 2014). موقع «بوليتيكو». مقال: «جون كيري: إدوارد سنودن هو «جبان... وخائن»».

Politico,
http://www.politico.com/story/2014/05/edward-snowden-coward-john-kerry-msnbc-interview-nsa-107157.html

89. فوييه غرينود (4 يوليو 2014). صحيفة الغارديان. مقال: «وفق كلينتون، يجب أن يحظى سنودن بالحق في الدفاع قانونياً عن نفسه في الولايات المتحدة».

Guardian,
http://www.theguardian.com/commentisfree/2014/may/30/daniel-ellsberg-snowden-fair-trial-kerry-espionageact.

Trevor Timm (23 Dec 2013), «If Snowden returned to US for trial, could court admit any NSA leak evidence?», *Boing Boing*,
http://boingboing.net/2013/12/23/snowden.html.

90. دانيال إلسبرغ (30 مايو 2014)، صحيفة الغارديان، مقال: «سنودن لن يحظى بمحاكمة عادلة، وكيري على خطأ».

Guardian,

<http://www.theguardian.com/commentisfree/2014/may/30/daniel-ellsberg-snowden-fair-trial-kerry-espionage-act>.

تريفور تيم (23 ديسمبر 2013). موقع «بوينغ بوينغ». مقال: «إذا عاد سنودن إلى الولايات المتحدة للمحاكمة، هل تقبل المحكمة أي دليل بصدد تسريبات «وكالة الأمن القومي»؟

Boing Boing,

<http://boingboing.net/2013/12/23/snowden.html>

91. نايت أندرسون (13 مايو 2014)، موقع «آرس تكنيكا». مقال: «كيف أدت رغبة عمدة في كشف مستخدم بذيء لـتويتر، إلى انفجار الأمر في وجهه».

Nate Anderson (13 May 2014), «How a mayor's quest to unmask a foul-mouthed Twitter user blew up in his face», *Ars Technica*, <http://arstechnica.com/tech-policy/2014/05/how-a-mayors-quest-to-unmask-a-foulmouthed-twitter-user-blew-up-in-his-face>
Kim Zetter (12 Jun 2014), «ACLU sues after Illinois mayor has cops raid guy parodying him on Twitter»,

Wired, <http://www.wired.com/2014/06/peoria-mayor-twitter-parody>

كيم زتر (12 يونيو 2014)، مجلة وايرد، مقال: «دعوى قضائية من «الاتحاد الأمريكي للحريات المدنية» عن عمدة «إلينوي» لأن شرطته أغارت على منزل أحد المتفاهرين على «تويتر».

Wired, <http://www.wired.com/2014/06/peoria-mayor-twitter-parody>.

92. جينا بورتنوي (19 مارس 2014). صحيفة نيويورك تايمس. مقال: «من المدعي العام إلى بوليس الولاية: توقف عن التقاط صور المحتجين في قاعة بلدية «كريس كريستي»».

New York Times,

<http://www.nytimes.com/2014/08/01/world/senate-intelligence-commitee-cia-interrogation-report.html>

93. لورا بواتراس ومارسيل روزنباخ وهولغر ستارك (26 أغسطس 2013). صحيفة دير شبيغل، مقال: «الاسم الشيفري هو «أبالاتشي»: كيف تجسست أميركا على أوروبا والأمم المتحدة».

Der Spiegel,

<http://www.spiegel.de/international/world/secret-nsa-documents-showhow-the-us-spies-on-europe-and-the-un-a-918625.html>

94. برايان روس وفيك فالتر وأنا شيشتر (9 أكتوبر 2008). شبكة «آيه بي سي نيوز». مقال: «داخل قصة التنصت على الأميركيين».

ABC News Nightline,

<http://abcnews.go.com/Blotter/exclusive-inside-account-us-eavesdropping-americans/story?id=5987804>.

95. سايروس فاريفار (17 يوليو 2014). موقع «آرس تكنيكا». مقال: «موظفو «وكالة الأمن القومي» تداولوا روتينياً صوراً عارية مأخوذة من مواد اعتراضها».

Ars Technica,

<http://arstechnica.com/tech-policy/2014/07/snowden-nsa-employees-routinely-pass-around-intercepted-nude-photos>.

96. سيوبهان غورمان (23 أغسطس 2013). صحيفة وول ستريت جورنال. مقال: «ضباط وكالة الأمن القومي، تجسّسوا أحياناً بدافع من الحب».

Wall Street Journal Washington Wire,

<http://blogs.wsj.com/washwire/2013/08/23/nsa-officers-sometimes-spy-on-love-interests>

97. وكالة الأمن القومي الأمريكية (3 مايو 2012). وثيقة: «تقرير داخلي فصلي عن الإشراف: الفصل الأول من العام 2012».

<http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB436/docs/EBB-044.pdf>.

98. تتعمّد «وكالة الأمن القومي» عدم أتمتة نظام التدقيق الداخلي، ما يعني أنها تستطيع أن تكتشف من التجاوزات بقدر عدد الأشخاص التي توكل إليهم تلك المهمة. مارسي ويلر (20 أغسطس 2013). مقال: «إذا ارتكبت «وكالة الأمن القومي» اعتداءات فاضحة على قاعدة بياناتها، ثم لم يكتشف أحد الأمر، سيكون قد حدث فعلياً؟». *Empty Wheel*,

<http://www.emptywheel.net/2013/08/20/if-nsa-commits-database-query-violations-but-nobodyaudits-them-do-they-really-happen>.

99. شوان آش (5 يناير 2012). موقع «ليتر أوف نوتس». رسالة: «وككل الفاسدين، إن نهايتك تقترب». *Letters of Note*,

<http://www.lettersofnote.com/2012/01/king-like-all-fraudsyour-end-is.html>

100. مجلس الشيوخ الأمريكي (26 أبريل 1976). وثيقة حكومية: «التقرير النهائي للجنة المنتدبة لدراسة عمليات الحكومة المتصلة بنشاطات الاستخبارات. الكتاب الثاني: نشاطات الاستخبارات وحقوق الأميركيين».

<https://archive.org/details/finalreportofsel02unit>

ميتشيل 02. شميذ وكولن موينيهان (24 ديسمبر 2012). صحيفة نيويورك تايمس. مقال: «وثائق تظهر أن عملاء الدِّافِ بي أي، لمكافحة الإرهاب، ترصدوا حركة احتلوا وول ستريت».

New York Times,

<http://www.nytimes.com/2012/12/25/nyregion/occupy-movement-was-investigated-by-fbi-counterterrorism-agents-records-show.html>

بو هوداي (9 يونيو 2013)، موقع «سورس ووتش». مقال: «رقابة الحكومة لـ«حركة احتلوا وول ستريت»». *Sourcewatch*,

http://www.sourcewatch.org/index.php/Government_Surveillance_of_Occupy_Movement.

102. شارلي سافاج وسكوت شاين (16 ديسمبر 2009). صحيفة نيويورك تايمس. مقال: «التجسس بطريقة مهينة على الأميركيين».

New York Times,

<http://www.nytimes.com/2009/12/17/us/17disclose.html>.

103. «الاتحاد الأمريكي للحريات المدنية» (25 أكتوبر 2006). وثيقة: «الاتحاد الأمريكي للحريات المدنية، يعرّي رقابة الدِّافِ بي أي، لنشطاء السلام في ولاية «ماين»».

<https://www.aclu.org/national-security/aclu-uncovers-fbi-surveillance-maine-peace-activists>

104. «الاتحاد الأمريكي للحريات المدنية» (29 يونيو 2010). وثيقة: «الرصد البوليسي لحرية التعبير: رقابة الشرطة وتدخله في نشاط يحميه التعديل الأول في الدستور».

https://www.aclu.org/files/assets/Spyfiles_2_0.pdf.

ليندا ي. فيشر (2004). مجلة «أريزوننا لور ريفيو». مقال: «الإبانة بالترابط التعبيري: التصنيف السياسي، الرقابة وخصوصية المجموعات».

Arizona Law Review 46,

<http://www.arizonalawreview.org/pdf/46-4/46arizrev621.pdf>.

US Department of Justice (Sep 2010), «A review of the FBI's investigations of certain domestic advocacy groups.»

<http://www.justice.gov/oig/special/s1009r.pdf>.

105. غلين غرينوالد ومرضى حسين (9 يوليو 2014). موقع «إنترسيت». مقال: «تحت الرقابة: لقاءات مع قادة أميركيين- مسلمين ترافقهم الدإف بي أي». وكالة الأمن القومي.

Intercept,

<https://firstlook.org/theintercept/article/2014/07/09/under-surveillance>

106. «وكالة أسوشيتد برس» (2012). مقال: «إضاءات من أداة للتحقيق الاستقصائي فائزة بجائزة «بوليتزر» للصحافة، على عمليات الرقابة التي يجريها بوليس نيويورك».

<http://www.ap.org/media-center/nypd/investigation>

, and <http://www.ap.org/Index/AP-In-The-News/NYPD>

107. كايد كروكفورد (25 مايو 2014). موقع «برايفسي إس أو إس». مقال: «وثائق تثبت أن مركز الاتصهار في بوسطن «المكافحة الإرهاب»، وثق «حركة احتلوا...» في بوسطن، بشكل وسواسي».

Privacy SOS,

<http://privacysos.org/node/1417>

كارول روز وكايد كروكفورد (30 مايو 2014)، مقال: «عندما تتجسس الشرطة على حرية التعبير، تعاني الديمقراطية».

<http://cognoscenti.wbur.org/2014/05/30/boston-regional-intelligence-center-carol-rosekade-crockford>.

108. لوك أونيل (13 أغسطس 2014). شبكة «آن بي سي نيوز». مقال: «الأخ الكبير» لـ«بينتان»: كيف استخدم بوليس مدينة بوسطن تقنية التعرف إلى الوجوه للتجسس على آلاف المشاركين في مهرجان موسيقي».

Noisey,

<http://noisey.vice.com/blog/beantowns-big-brother>

109. ليزا مايرز ونوغلاس باسترناك وريتش غارديلا (14 ديسمبر 2015). شبكة «آن بي سي نيوز». مقال: «هل يتجسس البنتاغون على أميركا؟»

Lisa Myers, Douglas Pasternak,

and Rich Gardella (14 Dec 2005), «Is the Pentagon spying on Americans?», *NBC News*,

http://www.nbcnews.com/id/10454316/ns/nbc-nightly_news_with_brian-williamsnbc_news_investigates/t/pentagon-spying-americans.

110. غلين غرينوالد وإراين غريم وإراين غالاهار (26 نوفمبر 2013). صحيفة هافنغتون بوست. مقال: «وثائق سرية جداً تظهر تجسس «وكالة الأمن القومي» على عادات مشاهدة أشرطة الجنس الإباحي، كجزء من خطة لإنقاذ «المجذرين» مصداقيتهم».

Huffington Post,

http://www.huffingtonpost.com/2013/11/26/nsa-porn-muslims_n_4346128.html

111. كريس هامبي (6 أكتوبر 2014). مقال: «الحكومة تستخدم اسم امرأة في صنع صفحة مزيفة على «فيسبوك»».

<http://www.buzzfeed.com/chrishamby/government-says-federal-agents-can-impersonate-woman-online>

112. وليام بندر (23 فبراير 2010). صحيفة فيلادلفيا إنكوايرر. مقال: «نقلًا عن حماني: ل. ماريون صامت بصدد عدد من الصور الملتقطة بكاميرا الدويب».

Philadelphia Inquirer,

http://articles.philly.com/2010-02-23/news/24957453_1_webcam-laptops-students

113. إريك ليشتبلاو وجيمس ريزن (23 يونيو 2006). صحيفة نيويورك تايمس. مقال: «تلاعبت الولايات المتحدة سرًا ببيانات البنوك بذريعة محاربة الإرهاب».

New York Times,

<http://www.nytimes.com/2006/06/23/washington/23intel.html>.

لويك إيسر (3 يوليو 2014). مجلة عالم الكمبيوتر. مقال: «محكمة «الاتحاد الأوروبي» تطالب بشفافية أكبر في البرنامج الأمريكي- الأوروبي لتتبع أموال الإرهاب».

PC World,

<http://www.pcworld.com/article/2450760/eu-court-orders-more-transparency-over-useu-terrorist-finance-tracking-program.html>

مونيكار إرميت (23 أكتوبر 2013). مقال: «البرلمان الأوروبي: لا استمرار في نقل بيانات البنوك إلى التحقيقات الأميركية عن الإرهاب».

Intellectual Property Watch,

<http://www.ip-watch.org/2013/10/23/european-parliament-no-more-bank-data-transfers-to-us-for-anti-terror-investigations>

114. «الاتحاد الأمريكي للحريات المدنية». (7 مارس 2002). تقرير: «كيف يعزّز قانون باتريوت، تفويضات تسلّل وتلصص، المعطاة إلى قوى إنفاذ القانون».

<https://www.aclu.org/technologyand-liberty/how-usa-patriot-act-expands-law-enforcement-sneak-and-peek-warrants>.

تيم تريפור (26 أكتوبر 2011). «مؤسسة الحدود الإلكترونية». مقال: «بعد عشر سنوات على قانون باتريوت، عرض للتشريعات الثلاثة الأكثر مساساً بحياة المواطنين الأميركيين العاديين».

Electronic Frontier Foundation,

<https://www.eff.org/deeplinks/2011/10/ten-years-later-look-three-scariestprovisions-usa-patriot-act>.

115. تتشارك «وكالة الأمن القومي» المعلومات مع «وكالة مكافحة المخدرات» منذ سبعينيات القرن العشرين. جيمس بامفورد (2008)، كتاب: المصنع الخفي: وكالة الأمن القومي الفائقة الخفاء من 11/9 إلى التنصت على أميركا. دار «دوبلداي» للنشر.

The Shadow Factory: The

Ultra-Secret NSA from 9/11 to Eavesdropping on America, Doubleday,

<http://books.google.com/books?id=8xJmxWNTxrwC>

116. جون شيفمان وكريستينا كوك (5 أغسطس 2013). وكالة «رويترز» للأنباء. مقال: «الحكومة توجّه عملاء بإخفاء برنامج استُخدِم في التحقيق مع أميركيين».

Reuters,

<http://www.reuters.com/article/2013/08/05/us-dea-sod-idUSBRE97409R20130805>

هاني فاخوري (6 أغسطس 2013). «مؤسسة الحدود الإلكترونية». تقرير: «تشارك في البيانات بين وكالة الأمن القومي» و«وكالة مكافحة المخدرات»، يؤدي إلى استعمال معلومات الرقابة في التحقيقات العادية».

Electronic Frontier Foundation,

<https://www.eff.org/deeplinks/2013/08/dea-and-nsa-team-intelligence-laundring>.

John Shiffman and David Ingram (7 Aug 2013), «IRS manual detailed DEA's use of hidden intel evidence», Reuters,

<http://www.reuters.com/article/2013/08/07/us-deairs-idUSBRE9761AZ20130807>.

117. قدّم مُطلق صافرة الإنذار بيل بيني الوصف التالي: «... عندما لا تتمكن من استعمال البيانات، يجب عليك صنع بنية موازية [ما يعني] أنك تستعمل ما تعدّه وسائل تحقيق عادية، [ثم] تعثر على البيانات. لكنك تملك تلميحاً معيّناً. إذ أخبرتك «وكالة الأمن القومي» أين توجد تلك البيانات...» أليكس أويراين (30 سبتمبر 2014). تقرير: «مدير متقاعد للتكنولوجيا في «وكالة الأمن القومي» يشرح وثائق سنودن».

<http://www.alexao'Brien.com/second sight/wb/binney.html>

118. برايان كريس (14 أكتوبر 2014). موقع «كريس أو سكيوريتي». مقال: «محامو «درب الحرية» يجدون ثغرات في رواية الدوافع بي أي».

Krebs on Security,

<http://krebsonsecurity.com/2014/10/silk-road-lawyers-poke-holes-in-fbis-story>

119. روب إيفانز وبول لويس (26 أكتوبر 2009). صحيفة الغارديان. مقال: «تحدي قوات الشرطة بشأن صنع ملفات عن محتجين ملتزمين بالقوانين».

Guardian,

<http://www.theguardian.com/uk/2009/oct/26/police-challenged-protest-files>

120. غوردون راينر وريتشارد ألكلياني (12 أبريل 2008). صحيفة التلغراف. مقال: «حالات تجسس المجلس تلامس الألف شهرياً».

Telegraph,

<http://www.telegraph.co.uk/news/uknews/1584808/Council-spy-cases-hit-1000-a-month.html>

سارة ليول (24 أكتوبر 2009). صحيفة نيويورك تايمس. مقال: «ارتياح البريطانيين من الرقابة على القضايا الصغيرة».

New York Times,

<http://www.nytimes.com/2009/10/25/world/europe/25surveillance.html>

121. جيمس بامفورد (16 سبتمبر 2014). صحيفة نيويورك تايمس. مقال: «فضيحة إسرائيل ووكالة الأمن القومي».

New York Times,

<http://www.nytimes.com/2014/09/17/opinion/israels-nsa-scandal.html>

122. هناك مقال يثير تلك النقطة تحديداً. دانيال دايقيس (23 سبتمبر 2014). مقال: «كل شخص يعمل في المعلوماتية، وكل مدير...».

<http://crookedtimber.org/2014/09/23/every-single-it-guy-every-single-manager>

123. هيلاري رودهام كلينتون (21 يناير 2010)، خطاب «حرية الإنترنت». مجلة فورين بوليسي.

Foreign Policy,

http://www.foreignpolicy.com/articles/2010/01/21/internet_freedom

124. وزارة الخارجية الأمريكية (2014). تقرير: «حرية الإنترنت».

<http://www.state.gov/e/eb/cip/netfreedom/index.htm>

125. هيئة الإذاعة البريطانية (2 يونيو 2014). مقال: «نحن مراقبون»، يقول المصريون على الدسوشال ميديا». *BBC News,*

<http://www.bbc.com/news/blogs-trending-27665568>.

126. جابشري باجورا (5 يونيو 2014). صحيفة إنديا ريبيل تايم. مقال: «سنودن وتلصص الهند».

India Real Time,

<http://blogs.wsj.com/indiarealtime/2014/06/05/indias-snoopingand-snowden>.

127. شانون تيزي (28 مارس 2014). موقع «ديبلومات». مقال: «الصين تتدّ بالنتفاق الأمريكي في التجسس السرياني».

<http://thediplomat.com/2014/03/china-decries-us-hypocrisy-on-cyber-espionage>

وكالة «شينخوا» للأنباء (11 يوليو 2014). صحيفة تشاينا دايلي. مقال: «بوتين يصف ممارسات الرقابة الأمريكية بأنها «نفاق كامل»».

China Daily,

http://www.chinadaily.com.cn/world/2014-07/11/content_17735783.htm

128. مارك زوكربيرغ (13 مارس 2014)، تدوين إلكتروني على «فيسبوك»: «العالم يقدو أكثر تعقيداً...».

Facebook,

<https://www.facebook.com/zuck/posts/10101301165605491>.

الفصل 8: العدالة التجارية والمساواة

1. «مكتب المدعي العام في «مينسوتا» (19 يناير 2012)، قضية: «المدعي العام سوانسون يقاضي «أكريفت هيلث» لانتهاكها خصوصية المرضى».
<http://www.ag.state.mn.us/Consumer/PressRelease/120119AccretiveHealth.asp>
2. توني كينيدي ومورا ليرنر (31 يوليو 2012)، صحيفة ستار تريبيون، مقال: «حظر «أكريفت» في «مينسوتا»».
Star-Tribune,
<http://www.startribune.com/lifestyle/health/164313776.html>.
3. كايت كراوفورد وجايسون شولتز (2014)، مجلة بوسطن كولينج لو ريفيو، ورقة: «بيانات ضخمة وعملية متلائمة معها: نحو إطار لتصحيح مخاطر الخصوصية التوقعية».
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2325784.
4. مارك هوكشتاين (26 يونيو 2000)، موقع «أميركان بانكر»، مقال: «بنك «ويلز فارغو» يمحو وصلة إلكترونية بعد مقاضاته من «أكرون»».
American Banker,
http://www.americanbanker.com/issues/165_119/-128168-1.html
غاري هيرنانديز وكاثارين ايدي وجويل ماتشمور (خريف 2001)، مجلة ساوثرن ميتوديست يونيفرستي لو ريفيو، ورقة: «ممارسة «عبر خطوط الويب» هي تمييز غير عادل في الفضاء السراني».
<http://heinonline.org/HOL/LandingPage?collection=journals&handle=hein.journals/smulr54&div=91>.
5. بيل دافيدو (5 مارس 2014)، مجلة آتلانتيك، مقال: «ممارسة «عبر الخطوط الحمراء» في القرن 21».
Atlantic,
<http://www.theatlantic.com/business/archive/2014/03/redlining-for-the-21st-century/284235>.
6. مايكل ليدتكة (22 يونيو 2000)، صحيفة لوس أنجلوس تايمس، مقال: «دعوى قضائية بشأن استخدام «ويلز فارغو» الإنترنت لترويج التمييز».
Los Angeles Times,
<http://articles.latimes.com/2000/jun/22/business/fi-43532>.
رونا أبرامسون (23 يونيو 2000)، مجلة عالم الكمبيوتر، مقال: «إدانة «ويلز فارغو» بممارسة سياسة «عبر الخطوط الحمراء» على الإنترنت».
Computer World,
<http://www.computerworld.com/article/2596352/financial-it/wells-fargo-accused-of--redlining--on-the-net.html>
7. مارسيا ستيبانيك (3 أبريل 2000)، مجلة بلومبرغ ويك، مقال: «عبر خطوط الويب».
كايسي جونستون (10 أكتوبر 2013)، موقع «أرس تكنيكا»، مقال: «هل رفض طلبك ذلك القرض؟ عليك أن تشكر جمع المعلومات على الدويب».
Ars Technica,
<http://arstechnica.com/business/2013/10/denied-for-that-loan-soon-you-may-thank-online-data-collection>.
8. «المكتب التنفيذي للرئاسة» (1 مايو 2014)، تقرير: «البيانات الضخمة: التقاط الفرصة والحفاظ على القيم».
http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.
9. يجب على «أوبر» تعديل أسعارها كي لا تتصادم مع قيود ولاية «نيويورك» التي تحظر رفع الأسعار أثناء حالات الطوارئ؛ مايك آيزاك (8 يوليو 2014)، صحيفة نيويورك تايمس، مقال: «التوصل إلى اتفاقية بين شركة «أوبر» وولاية نيويورك بشأن رفع الأسعار في أحوال الطوارئ».
New York Times,

<http://bits.blogs.nytimes.com/2014/07/08/uber-reaches-agreement-with-n-yon-surge-pricing-during-emergencies>.

بيتر ميلمر (12 أغسطس 2014). مجلة فوربس. مقال: «شركة «أوبر»: جيّدة تماماً، ولكن ليس كفاية».

Forbes,

<http://www.forbes.com/sites/peterhimler/2014/08/12/uber-socool-but-so-uncool>

10. جنيفر فالنتينو-دوفريز وجيرمي سنغير-فاين وأشكان سلطاني، وول ستريت جورنال. مقال: «مواقع شبكية تقدّم أسعاراً مختلفة في صفقات تعتمد على المعلومات عن المستخدم».

Wall Street Journal,

<http://online.wsj.com/news/articles/SB10001424127887323777204578189391813881534>.

Michael Schrage (29 Jan 2014), «Big data's dangerous new era of discrimination»,

Harvard Business Review,

<http://blogs.hbr.org/2014/01/big-datas-dangerous-new-era-of-discrimination>

11. إميلي سنيل وجوليا أنغوين (4 أغسطس 2010). صحيفة وول ستريت جورنال. مقال: «في الحدود القصوى لتقنيات الدوبيب»، ليس إغفال الهوية سوى اسم».

Wall Street Journal,

<http://online.wsj.com/news/articles/SB10001424052748703294904575385532109190198>

12. جنيفر فالنتينو-دوفريز وجيرمي سنغير-فاين وأشكان سلطاني، وول ستريت جورنال. مقال: «مواقع شبكية تقدّم أسعاراً مختلفة في صفقات تعتمد على المعلومات عن المستخدم».

Wall Street Journal,

<http://online.wsj.com/news/articles/SB10001424127887323777204578189391813881534>

13. بام ديكسون وروبرت غيلمان (2 أبريل 2014). «منتدى الخصوصية العالمي». مقال: «سجل لأميركا كزبون: كيف تهدّد السجلات السرية للمستهلك خصوصيتك ومستقبك».

World Privacy Forum,

http://www.worldprivacyforum.org/wp-content/uploads/2014/04/WPF_Scoring_of_America_April2014_fs.pdf

14. جيسكا فاسيلارو (7 مارس 2011). صحيفة وول ستريت جورنال. مقال: «الموجة المقبلة في التلفزة: ضبط الإرسال ليكون أنت».

Wall Street Journal,

<http://online.wsj.com/articles/SB10001424052748704288304576171251689944350>

15. دانا ماتيوالي (23 أغسطس 2012). صحيفة وول ستريت جورنال. مقال: «في «أوبرتز»، مستخدمو الدماك» يواجهون استضافة أعلى سعراً».

Wall Street Journal,

<http://online.wsj.com/news/articles/SB10001424052702304458604577488822667325882>

16. بيل ماكسي (3 أبريل 2013). صحيفة يو إس إيه توداي. مقال: «هل عروض السفر تتغيّر وفق تاريخ تصفحك للإنترنت؟»

USA Today,

<http://www.usatoday.com/story/travel/columnist/mcgee/2013/04/03/do-travel-deals-change-based-on-your-browsing-history/2021993>.

17. لوشيا موسيس (2 أكتوبر 2013). مجلة أد ويك. مقال: «يحرص المسوّقون على معرفة متى تشعر المرأة بأن جاذبيتها أقل: ما هي الرسائل التي يجب نقلها، ومتى يجب إرسالها».

Adweek,

<http://www.adweek.com/news/advertising-branding/marketers-should-take-note-when-women-feel-least-attractive-152753>.

Kim Bates (4 Oct 2013), «Beauty vulnerability: What got lost in translation», *Adweek*, <http://www.adweek.com/news/advertising-branding/beauty-vulnerabilitywhat-got-lost-translation-152909>

18. «فرانك ن. مجيد أسوسيتس» (2011). «رابطة صحف أميركا». مقال: «كيف تتسوق أميركا وتنفق في 2011». http://www.naa.org/docs/newspapermedia/data/howamericashopsandspends_2011.pdf

19. كاتي لوبيوسكو (27 أغسطس 2013). شبكة «سي أن أن». مقال: «قائمة أصدقائك على «فيسبوك»، تغير حسابك في بطاقة الائتمان».

CNN,

<http://money.cnn.com/2013/08/26/technology/social/facebook-credit-score>.

20. كاري تغردين (21 ديسمبر 2008). صحيفة أتلانتا جورنال-كونستيتيوشن. مقال: «شركات بطاقات الائتمان تغير سقوف بطاقتها: تكون أقل للبعض وفقاً لأمكنة مشترياتهم».

Atlanta Journal-Constitution,

https://web.archive.org/web/20110728060844/http://www.ajc.com/news/content/business/stories/2008/12/21/creditcards_1221.html

21. أوسكار غندي جونيور (1993). كتاب: الفرز بواسطة الرؤية الشاملة: الاقتصاد السياسي للمعلومات الشخصية. دار «ويست فيو برس».

The Panoptic Sort: A Political Economy of Personal Information, Westview Press,

<http://books.google.com/books?id=wreFAAAAMAAJ>.

22. ورقة البحث التالية تسرد الطرق المتنوعة التي تتبعها الشركات في التمييز استناداً إلى «البيانات الضخمة». سولون بروكاس وأندرو سلبست (14 سبتمبر 2014). «سوشال ساينس ريسرش نتورك». ورقة بحث: «التفاوت في تأثير «البيانات الضخمة»».

Social Science Research Network,

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2477899

23. كايسي جونسون (13 أغسطس 2014). موقع «أرس تكنيكا». مقال: «المطعم الذي فتشت عليه في «غوغل»، يستخدمه أيضاً في استخراج معلومات عنك».

Ars Technica,

<http://arstechnica.com/staff/2014/04/when-the-restaurant-you-googled-googles-you-back>

24. هيلاري أوزبورن (13 أغسطس 2012). صحيفة الغارديان. مقال: «شركة «أفيفا» للسيارات تجرّب تقنية التأمين بالهاتف الذكي».

Guardian,

<http://www.theguardian.com/money/2012/aug/13/aviva-trial-smartphone-car-insurance-technology>

راندال ستروس (25 نوفمبر 2012)، صحيفة نيويورك تايمس. مقال: «إذا كنت سائقاً ماهرأ، دعنا نقيم ذلك».

New York Times,

<http://www.nytimes.com/2012/11/25/business/seeking-cheaper-insurance-driversaccept-monitoring-devices.html>.

براد توتيل (6 أغسطس 2013). مجلة تايم. «السائق المساعد هو «البيانات الضخمة»: شركات ضمان السيارات تروج أدوات ترصد عادات القيادة».

Time,

<http://business.time.com/2013/08/06/big-data-is-my-copilot-auto-insurers-push-devices-that-track-driving-habits>.

25. نانسي غورينغ (7 يوليو 2017). موقع «ساست ورلد». مقال: «هذه الشركة وقّعت ثلاثمائة ألف دولار من أموال الضمان الصحي، بإعطاء موظفيها سوارات «فت بت»».

CiteWorld,

<http://www.citeworld.com/article/2450823/internet-of-things/appirio-fitbit-experiment.html>

26. لي كراين (5 سبتمبر 2013). مجلة ديجيتال تريفيدي. مقال: «درس الرياضة سيصبح أسوأ لغير محبي الرياضة».

Digital Trends,

<http://www.digitaltrends.com/sports/gym-class-is-about-to-get-even-worse-for-the-athletically-disinclined>

إميلي ميلز (28 مايو 2014). موقع «ليدر - تلغرام». مقال: «طلاب ثانوية «ميموريال» بلغوا ذروة لياقتهم بفضل مجسات لنشاط القلب».

Leader-Telegram,

http://www.leadertelegram.com/news/front_page/article_ec2f0b72-e627-11e3-ac95-0019bb2963f4.html

Katie Wiedemann (14 Aug 2014), «Heart rate monitors now required in Dubuque

P.E. classes», KCRG,

<http://www.kcrg.com/subject/news/heart-rate-monitors-nowrequired-in-dubuque-physical-education-classes-20140814>

27. جويل شيشتمان (14 مارس 2012). صحيفة وول ستريت جورنال. مقال: «سجل: برنامج من شركة «أنتش بي» استطاع التنبؤ بالموظفين المشوكة على ترك الشركة».

Wall Street Journal,

<http://blogs.wsj.com/cio/2013/03/14/book-hp-piloted-program-to-predict-which-workers-would-quit>

28. تعطي الورقة التالية تحليلاً ممتازاً للرقابة في مواقع العمل. أليكس روكسنبلات وتامارا كنزي ودانا بويد (8 أكتوبر 2014). موقع «داتا أند سوسيتي ريسيرتش إنستيتيوت».

Data and Society Research Institute,

<http://www.datasociety.net/pubs/fow/WorkplaceSurveillance.pdf>

29. إلين مسمير (31 مارس 2010). موقع «نتورك ورلد». مقال: «هل تحس أنك مراقب في العمل؟ الأرجح أنك محق».

Network World,

<http://www.networkworld.com/article/2205938/data-center/feel-like-you-re-being-watched-at-work--youmay-be-right.html>

جوش بيرسن (25 يونيو 2014). مجلة فوربس. مقال: «الذات المقومة كميًا: نتحدث عن الموظف المقوم كميًا».

Forbes,

<http://www.forbes.com/sites/joshbersin/2014/06/25/quantified-self-meet-the-quantified-employee>

30. دون بيك (20 نوفمبر 2013). مجلة أتلانتيك. مقال: «إنهم يراقبونك في العمل».

Atlantic,

<http://www.theatlantic.com/magazine/archive/2013/12/theyre-watching-you-at-work/354681>

هانا كوشلر (17 فبراير 2014). صحيفة فايننشال تايمس. مقال: «رؤاد التقنية يراقبوننا في العمل».

Financial Times,

<http://www.ft.com/intl/cms/s/2/d56004b0-9581-11e3-9fd6-00144feab7de.html>

31. يعتبر المقال التالي مراجعة ممتازة عن تقنيات الرقابة في أمكنة العمل وتأثيراتها في الخصوصية. كوري أ. سيوشيتي (2010). جامعة دنفر. بحث: «رب العمل المتنصت: إطار للقرن 21 عن ترصد الموظف».

University of Denver,

http://www.futureofprivacy.org/wp-content/uploads/2010/07/The_Eavesdropping_Employer_%20A_Twenty-First_Century_Framework.pdf

32. حدثتني إحدى الصديقات عن مشاعرها حيال الإعلان المُشخص. قالت إنها امرأة متقدمة في السن، وتلقى باستمرار إعلانات عن عمليات تجميل، أدوية لعلاج أمراض «الكبار» وأشياء أخرى تذكرها دوماً بعمرها. وتجد ذلك غير مريح. لين سودبري وبيتر سيمكوك (2008). مقال: «تابو كبار السن؟ إعلانات مستندة إلى العمر، النظرة الذاتية إلى العمر والمستهلك الكبير السن».

European Advances in Consumer Research 8,

http://www.acrwebsite.org/volumes/eacr/vol8/eacr_vol8_28.pdf.

33. ديبورا س. بيل (7 فبراير 2014). «إعلان د. ديبورا س. بيل «مؤسسة حقوق الخصوصية للمرضى» بدعم من استجواب المدعين للحصول على ملخص جزئي للحكم». في «قضية الكنيسة التوحيدية الأولى وفريقها ضد وكالة الأمن القومي» وفريقها، في محكمة المقاطعة الشمالية في كاليفورنيا.

<https://www.eff.org/files/2013/11/06/allplaintiffsdeclarations.pdf>.

34. أندرو أولديزكو (-5 يونيو 2014). «مؤتمر بحثة قوانين الخصوصية» في واشنطن. بحث: «نهاية الخصوصية ويزور دمار الرأسمالية».

<http://www.law.berkeley.edu/plsc.htm>

35. 713 بادي كامن (5 يوليو 2001). صحيفة تورنتو ستار. مقال: «هل اعتقدت بأن محركات البحث تقدم نتائج محايدة؟ فكر ثانية».

<http://www.commercialalert.org/issues/culture/search-engines/so-you-thought-search-engines-offer-up-neutralresults-think-again>

36. غاري روسكين (16 يوليو 2001). رسالة إلى دونالد كلارك، «اللجنة الفيدرالية للتجارة»: عن «شكوى بالتلاعب الإعلاني ضد شركات «ألفايسستا»، «إيه أو آل تايم ورنر»، «دايركت هت تكنولوجيايز»، «أي وون»، «لوك سمارت»، «مايكروسوفت» و«تيرا لايكوس».

<http://www.commercialalert.org/PDFs/SearchEngines.pdf>

هيثر هيسلي (27 يونيو 2002). رسالة إلى غاري روسكين، عن: شكوى تطلب التحقيق مع شركات محركات البحث على الإنترنت بشأن الموضوعة المدفوعة وبرامج الاشتغال المدفوعة. «اللجنة الفيدرالية للتجارة».

Commission,

http://www.ftc.gov/sites/default/files/documents/closing_letters/commercial-alert-response-letter/commercialalertletter.pdf

37. داني سوليفان (30 مايو 2012). موقع «ماركيتنغ لاند». مقال: «بعد أن عُدَّها شيطاناً، بات «غوغل» يتبنى «الاشتغال المدفوع»».

Marketing Land,

<http://marketingland.com/once-deemed-evil-google-now-embraces-paid-inclusion-13138>

38. مايكل كوني (25 يونيو 2013). موقع «نتورك ورلد». مقال: «طلبت «اللجنة الفيدرالية للتجارة» من «غوغل» و«ياهو» و«بينغ» وغيرهم، تحسين طريقة تمييز الإعلانات في نتائج تفتيش المحتوى على الإنترنت».

Network World,

<http://www.networkworld.com/community/blog/ftc-tells-google-yahoo-bingothers-better-differentiate-ads-web-content-searches>

ماري ي. أنغل (24 يونيو 2013). «اللجنة الفيدرالية للتجارة». «رسالة قضائية عن: ممارسات الإعلان على محركات البحث».

<http://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-consumerprotection-staff-updates-agencys-guidance-search-engine-industryon-need-distinguish/130625searchenginegeneralletter.pdf>

39. جوش كونستين (3 أكتوبر 2012). موقع «تيك كرانش». مقال: «رأهنا، صار «فيسبوك» يتيح للمستخدمين الأميركيين دفع 7 دولارات مقابل إصالح تدويناتهم إلى عدد أكبر من الأصدقاء».

Tech Crunch,

<http://techcrunch.com/2012/10/03/us-promoted-posts>

40. روبرت بوند وآخرون (13 سبتمبر 2012). مجلة نايتشر العلمية. بحث: «وضع 61 مليون شخص قيد تجربة في التأثير الاجتماعي والتشديد السياسي».

Nature 489,

<http://www.nature.com/nature/journal/v489/n7415/full/nature11421.html>

41. استقصى جوناثان زيترين ذلك الاحتمال. جوناثان زيترين (1 يونيو 2014). موقع «نيو ريپبليك». مقال: «يستطيع «فيسبوك» أن يحسم الانتخابات من دون أن يلاحظه أحد».

New Republic,

<http://www.newrepublic.com/article/117878/information-fiduciary-solution-facebook-digital-gerrymandering>

42. كانت مجموعة من الانتخابات الأميركية متقاربة. ويفارق 0.01 % من الأصوات، كان آل غور ليفوز على جورج بوش في 2000. وفي 2008، كان آل فرانكلين ليهزم نورمان كولمان في انتخابات مقعد مجلس الشيوخ عن ولاية «مينسوتا»، لو تغير اتجاه 312 صوتاً.

43. 721 روبرت إيبشتاين (مايو 2013). مقال: «ديموقراطية في خطر: التلاعب بنتائج البحث على الإنترنت، بإمكانه تغيير تفضيلات المصوتين دون أن يدروا».

25th Annual Meeting of the Association for Psychological Science, Washington, D.C.,

http://aibrt.org/downloads/EPSTEIN_and_Robertson_2013-Democracy_at_Risk-APS-summary-5-13.pdf

44. «عندما تكون كمية المعلومات فائقة الضخامة والشفافية والاختراق؛ لا يلزمك إطلاقاً سوى استعمال الحقائق المثبتة لاختراق في بروباغندا مطلقة وتحويل الناس إلى قطعان كلياً». اقتباس من دان غير نقله جوناثان زيترين (20 يونيو 2014)، مجلة منتدي هارفرد للقانون، بحث: «انتخابات مخططة».

Harvard Law Review Forum 127,

<http://harvardlawreview.org/2014/06/engineering-an-election>

45. آي وي وي وي (17 أكتوبر 2012). موقع «نيوستاتس مان». مقال: «مجاميع الصين المدفوعة الأجر: حزب الخمسين سنتاً».

New Statesman,

<http://www.newstatesman.com/politics/politics/2012/10/china%E2%80%99s-paid-trolls-meet-50-cent-party>

غاري كينغ وجنيفر بان ومارغريت ي. روبرتس (22 أغسطس 2014). مجلة ساينس العلمية. بحث: «الحجب بواسطة التخطيط المعكوس: اختبار عشوائي وملاحظة المشارك».

Science 345,

<http://www.sciencemag.org/content/345/6199/1251722>.

46. فيليب إلر- ديوييت (16 إبريل 2013). مجلة فورتن. مقال: «تدعي «سامسونغ» أنها ليست كذلك».

Fortune,

<http://fortune.com/2013/04/16/say-it-aint-so-samsung>

47. برايان هورلينغ وماثيو كوليك (4 ديسمبر 2009)، «المدونة الإلكترونية الرسمية لـ«غوغل»»، مقال: «بحث مُشخص للجميع».

Google Official Blog,

<http://googleblog.blogspot.com/2009/12/personalized-search-for-everyone.html>

تيم آدمز (19 يناير 2013)، صحيفة الغارديان، مقال: «محرك غوغل» ومستقبل البحث: أميت سنغال والرسم البياني للمعرفة.

Guardian,

<http://www.theguardian.com/technology/2013/jan/19/google-search-knowledge-graph-singhal-interview>

48. «شبكة شيكيتا الإلكترونية للإعلان» (7 يناير 2013). مقال: «قيمة الموضحة في نتائج «غوغل»».
<https://cdn2.hubspot.net/hub/239330/file-61331237-pdf/ChitikaInsights-ValueofGoogleResultsPositioning.pdf>

49. جوزيف تورو (2013). كتاب: أنت اليومي: الصناعة الجديدة للإعلانات تحدّد هويتك وقيمته. «مطبعة جامعة يال».

<http://yalepress.yale.edu/yupbooks/book.asp?isbn=9780300165012>

50. إيلي بارينز (2011)، كتاب: فقاعة الفلتر: ما الذي تخفيه الإنترنت عنك؟. كتب «بنغوين».
<http://www.thefilterbubble.com>.

51. كاس زونشتاين (2009). كتاب: الجمهورية. كوم، 2.0. مطبعة جامعة برنستون.
<http://press.princeton.edu/titles/8468.html>

52. للإنصاف، ذلك الميل أكثر قدماً وعمومية من الإنترنت. روبرت د. بوتمان (200)، كتاب: لعب البوليفينغ وحيداً: انهيار المجتمع الأمريكي وتجدده. «دار سايمون وشوستر».

<http://bowlingalone.com>

53. آدم د. أي. كرامر وجايمي ي. غولوري وجيفري ت. هانكوك (17 يونيو 2014). بحث: «دلائل تجريبية عن حدوث عداوات عاطفية ضخمة بواسطة شبكات التواصل الاجتماعي».

Proceedings of the National Academy of Sciences of the United States of America 111,

<http://www.pnas.org/content/111/24/8788.full>

54. لوشيا موسيس (2 أكتوبر 2013). مجلة آد ويك. مقال: «يحرص المسوّقون على معرفة متى تشعر المرأة بأن جاذبيتها أقل: ما هي الرسائل التي يجب نقلها، ومتى يجب إرسالها».

Adweek,

<http://www.adweek.com/news/advertising-branding/marketers-should-take-note-when-women-feel-least-attractive-152753>.

55. مارك بوكمان (17 أغسطس 2007). مجلة ستراتيجي + بيزنس. مقال: «علم الإشارات المرفهة».

strategy+business magazine,

http://web.media.mit.edu/~sandy/Honest-Signals-sb48_07307.pdf

56. يملك ذلك التلاعب كله إمكان كامنة بإحداث ضرر أكبر بواسطة الإنترنت؛ لأن تركيبة مجتمعنا بعد ذاتها تتحكم بها الشركات. كتب البروفيسور ريتشارد ليسينغ، وهو أستاذ قانون في «جامعة هارفرد» عن بنية الحوسبة بوصفها أداة للسيطرة. لورانس ليسينغ (2006). كتاب: الشيفرة: القوانين الأخرى للقضاء السبراني، نسخة 2.0. دار «بازيك بوكس».

<http://codev2.cc>

57. إد بلنكنغتون وأماندا ميشيل (17 فبراير 2012)، صحيفة الغارديان، «أوباما و«فيسبوك» وقوة الصداقة: البيانات في حملة 2012 الانتخابية».

Guardian,

<http://www.theguardian.com/world/2012/feb/17/obama-digital-data-machinefacebook-election>

تأزينا فيفا (20 فبراير 2012)، صحيفة نيويورك تايمس، «بيانات شبكية ساعدت في توجيه الإعلانات في حملة 2012 الانتخابية».

New York Times,

<http://www.nytimes.com/2012/02/21/us/politics/campaigns-use-microtargeting-to-attract-supporters.html>

ناثان آبز (أكتوبر 2012). «تأثير البيانات الضخمة» في مآل الحملات السياسية: الإعلان السياسي الموجه إلى مجموعات ميكروية في انتخابات الرئاسة للعام 2012.

Interactive Advertising Bureau,

http://www.iab.net/media/file/Innovations_In_Web_Marketing_and_Advertising_delivery.pdf

58. ساشا آيزنبرغ (19 ديسمبر 2012). موقع «إم أي تي» تكنولوجي ريفيو، مقال: «كيف استعملت حملة الرئيس أوباما «البيانات الضخمة» في تعبئة الناخب الفرد».

MIT Technology Review,

<http://www.technologyreview.com/featuredstory/509026/how-obamas-team-used-big-data-to-rally-voters>

59. ميكاه آلتمان وكارين ماكdonald وميتشل ماكdonald (2005). «من يعيدون تقسيم المناطق الانتخابية بكسبة زر: كيف غيرت الحوسبة إعادة ترسيم المقاطعات». من كتاب: في الخطوط الحزبية: المنافسة، المحازبة وإعادة ترسيم المقاطعات في انتخابات الكونغرس، تأليف: توماس إي. مان وبروس إي. كاين. مطابع مؤسسات بروكينغز.

<http://openscholar.mit.edu/sites/default/files/dept/files/pushbutton.pdf>

ترايسي يان (23 يناير 2013)، صحيفة بوسطن غلوب، مقال: «تحويل الخريطة السياسية سلاحاً حزبياً».

Boston Globe,

<http://www.bostonglobe.com/news/nation/2013/06/22/new-district-maps-reaped-rewards-for-gop-congress-but-cost-fewer-moderates-more-gridlock/B6jCugm94tpBvVu77ay0wJ/story.html>

60. أرش بدينغتون (9 أكتوبر 2013). مؤسسة «فريدم هاوس». مقال: «لتجديد الديمقراطية الأمريكية، أزيلوا إعادة تخطيط المناطق الانتخابية».

Freedom House,

<http://www.freedomhouse.org/blog/renew-american-democracy-eliminate-gerrymandering>

برس ميلان (20 يوليو 2014). صحيفة نيوز أويرفر. مقال: «إعادة تخطيط المناطق الانتخابية في نورث كارولينا، خسارة للديمقراطية».

<http://www.newsobserver.com/2014/07/20/4014754/with-nc-gerrymandering-democracy.html>

61. جون ماركوف (16 فبراير 1995). صحيفة نيويورك تايمس. مقال: «القبض على اللص السراني الأكثر خطورة في دواخل شبكته الخاصة».

New York Times,

<http://www.nytimes.com/1995/02/16/us/a-most-wanted-cyberthief-is-caught-in-his-own-web.html>

62. روبرت أوهارو جونيور (17 فبراير 2005). صحيفة واشنطن بوست. مقال: «السطو على هويات في شركة».

Washington Post,

<http://www.washingtonpost.com/wp-dyn/articles/A30897-2005Feb16.html>

63. براين كريس (2 سبتمبر 2014). موقع «كريس أون سيكيوريتي». مقال: «بنوك: السطو على بطاقات ائتمان في «هوم دييو»».

Krebs on Security,

<http://krebsonsecurity.com/2014/09/banks-credit-card-breach-at-home-depot>

64. دومينيك روش (3 أكتوبر 2014). صحيفة الغارديان. مقال: «بنك «جي بي مورغان» يكشف عملية اختراق كبرى لبياناته، تؤثر في 76 مليون أسرة».

Guardian,

<http://www.theguardian.com/business/2014/oct/02/jp-morgan-76m-households-affected-data-breach>

65. براين كريس (20 أكتوبر 2013)، موقع «كريس أون سيكيوريتي». مقال: «شركة «إيكسبيريان» باع بيانات هويات، استخدمت في سرقة».

Krebs on Security,

<http://krebsonsecurity.com/2013/10/experian-sold-consumer-data-to-id-theft-service>.

66. م. ي. كابي (2008). كتاب: موجز لتاريخ جريمة الكمبيوتر: مقدمة للطلبة. جامعة نورويتش.

<http://www.mekabay.com/overviews/history.pdf>.

67. أضحت تلك الظاهرة مشكلة كبرى في الولايات المتحدة. مايكل كراينش (16 فبراير 2014)، صحيفة بوسطن غلوب. مقال: «بات» دائرة المداخل الداخلية، مثقلة بجرائم سرقة الهوية».

Boston Globe,

<http://www.bostonglobe.com/news/nation/2014/02/16/identity-theft-taxpayer-information-major-problem-for-irs/7SC0BarZMDvy07bbhDXwvN/story.html>.

SteveKroft (21 Sep 2014)

68. في العام 2014، عرفنا أنَّ «هاكرز» صينيين اخترقوا قاعدة بيانات تحتوي أسماء حملة الأذونات الأمنية في أميركا. لا نعلم إن كانوا يبحثون عن معلومات تساعد على ارتكاب جرائم، أم إنهم موظفون في الاستخبارات الحكومية يهدفون للضغط على أشخاص في مواقع نافذة. مايكل س. شميدت وديفيد ي. سانغر ونيكول بيلروث (9 يوليو 2014). صحيفة نيويورك تايمس. «هاكرز» صينيون يسعون خلف معلومات أساسية عن موظفين أميركيين».

New York Times,

<http://www.nytimes.com/2014/07/10/world/asia/chinese-hackers-pursue-key-data-on-us-workers.html>.

69. لنعط مجرد نموذج عن ذلك. أصاب برنامج خبيث الحواسيب في ما يزيد على 1000 شركة في العام 2014، وسطا على أرقام حسابات بنكية. لم تعرف شركات كثيرة أنها كانت من الضحايا.

نيكول بيلروث (8 سبتمبر 2014). صحيفة نيويورك تايمس. مقال: «اختراق بيانات «هوم ديبو» ربما الأضخم حتى الآن».

New York Times,

<http://bits.blogs.nytimes.com/2014/09/08/home-depot-confirms-that-it-was-hacked>

70. ريتشارد وينتون (1 سبتمبر 2011). صحيفة لوس أنجلوس تايمس. مقال: «الابتزاز الجنسي»: السجن 6 سنوات للدهاكر، الذي أوقع بالنساء والفتيات».

Los Angeles Times,

<http://latimesblogs.latimes.com/lanow/2011/09/sextortion-six-years-for-oc-hacker-whoforced-women-to-give-up-naked-pics-.html>.

71. نايت أندرسون (10 مارس 2013) موقع «أرس تكنيكا». مقال: «مقابلة مع الرجل الذي تجسّس على نساء بواسطة كاميراتهن الشبكية».

Ars Technica,

<http://arstechnica.com/tech-policy/2013/03/rat-breeders-meet-the-men-who-spy-on-women-through-their-webcams>.

72. كشمير ميل (25 سبتمبر 2012). مجلة فوربس. مقال: «لجنة التجارة الفيدرالية» أن شركات بيع حواسيب بالتقسيط التقطت صوراً لأزواج أثناء ممارسة الجنس».

Forbes,

<http://www.forbes.com/sites/kashmirhill/2012/09/25/ftc-its-not-cool-to-put-spyware-on-rent-to-own-computers-without-customer-consent>

دارا كير (22 أكتوبر 2013). شبكة «سي نت». مقال: «تسوية قضية شركة «أرون» لبيع الحواسيب بالتقسيط، مع «لجنة التجارة الفيدرالية» بشأن التجسس».

CNET,

<http://www.cnet.com/news/aarons-computer-rental-chain-settles-ftc-spying-charges>

الفصل 9: التنافسية التجارية

1. يورد الكتاب أن حقوقه تعود إلى العام 1994، لكنه طُبِعَ في أكتوبر 1993. بروس شنابر (1994)، كتاب: *التشفير التطبيقي: بروتوكولات العمل، والخوارزميات، وشيفرة المصدر في برنامج «سي»*.
<https://www.schneier.com/book-applied.html>
2. مجلة وايرد (أبريل 1996). مقال: «في الأكشاك الآن: كاتالوغ التشفير».
Wired,
<http://archive.wired.com/wired/archive/4.04/updata.html>.
3. ستيفن ت. وولكر (12 أكتوبر 1993). «شهادة شفوية من ستيفن ت. وولكر، رئيس شركة تراسنت إنفورميشن سيستمز»، أمام «لجنة العلاقات الخارجية» في مجلس النواب.
http://fas.org/irp/congress/1993_hr/931012_walker_oral.htm.
4. في ما يلي بعض المصادر عن قصص ربع مماثلة ما زالت جارية. آلين ناكاشيما (26 يوليو 2014). صحيفة واشنطن بوست. مقال: «تكاثر خدمات الاتصال الجديدة بواسطة الإنترنت، يعيق عمل قوى إنفاذ القانون».
Washington Post,
http://www.washingtonpost.com/world/national-security/proliferation-of-new-online-communications-services-poses-hurdles-for-law-enforcement/2014/07/25/645b13aa-0d21-11e4-b8e5-d0de80767fc2_story.html.
أورين كير (19 سبتمبر 2014). صحيفة واشنطن بوست. مقال: «لعبة «أبل» الخطيرة».
Washington Post,
<http://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/>
برنت كيندال (25 سبتمبر 2014). صحيفة وول ستريت جورنال. مقال: «مدير الدوافع بي أي» يثير مخاوف بشأن الهواتف الذكية».
Wall Street Journal,
<http://online.wsj.com/articles/fbi-director-raises-concerns-about-smartphone-security-plans-1411671434>
5. صاغ لويس فرييه، مدير الدوافع بي أي، المسألة على النحو التالي: «نحن نؤيد التشفير القوي المتناسك. إذ تحتاجه البلاد وصناعاتها. كل ما نريده هو مجرد وجود باب مصيدة يكون مفتاحه بيد قاضٍ، فندخل منه في حال خطأ أحدهم جريمة». وظهر اقتباس مماثل من مستشار الدوافع بي أي، في الفصل 6 من هذا الكتاب. بروك ن. مبيكس (12 مايو 1995). «الاقترام من باب المخدرات والإرهاب في التشفير».
<http://www.cyberwire.com/cwd/cwd.95.05.12a.html>
6. واين مادسن (نوفمبر 1994). «إشكالية الدكليس».
<http://www.sciencedirect.com/science/article/pii/S1353485894900973>.
7. مات بليز (9 ديسمبر 2011). «مفتاح المتعهد من مسافة آمنة: استعادة لتجربة «كليس شيب»».
<http://www.crypto.com/papers/escrow-acsc11.pdf>
8. امترك الجيش الأمريكي شيئاً مُشابهاً من صنع «وكالة الأمن القومي» منذ 1987، حمل اسم «إس تي يو-3».
«مؤسسة الأمن العسكري» (فبراير 1997). «كليب «إس تي يو-3»».
<http://www.tscm.com/STUIIIhandbook.html>
9. هال أبلسون وآخرون (يونيو 1999). مقال: «مخاطر استعادة المفتاح، مفتاح المتعهد والتشفير الموثوق من طرف ثالث».
<https://www.schneier.com/paper-key-escrow.html>
10. «متحف كريبتو» (2014). «المُشَقَّر «تي أس دي»-3600 «إي» من «إيه تي أند تي»».
<http://www.cryptomuseum.com/crypto/att/tsd3600>
11. دوروثي ي. كينغ ودينس ك. برانشاد (مارس 1996). «تصنيف نُظُم التشفير مع مفتاح المتعهد».
<http://faculty.nps.edu/dedennin/publications/Taxonomy-CACM.pdf>
12. لورانس هوفمان (10 يونيو 1999). «التطوير المتواصل لمنتجات بتشفير قوي يتنافس القوانين الأميركية للتصدير».
<http://cryptome.org/cpi-survey.htm>

12. يصف المقال التالي تلك الأزمنة. ستيفن ليفي (مايو 1993). مجلة وايرد. مقال: «متمردو التشفير».
Wired,
http://archive.wired.com/wired/archive/1.02/crypto.rebels_pr.html.
13. ناقش المقال التالي الملامح الثلاثة لتلك الخسائر. دانيال كاميل (29 يوليو 2014). «خسائر الرقابة: تأثير وكالة الأمن القومي» في الاقتصاد، حرية الإنترنت والفضاء السبراني.
http://www.newamerica.net/publications/policy/surveillance_costs_the_nsa_impact_on_the_economy_internet_freedom_cybersecurity
14. بارتون غيلمان ولورا بوارتراس (7 يونيو 2013). صحيفة واشنطن بوست. مقال: «الاستخبارات البريطانية والأمريكية تنقب في بيانات 9 شركات أمريكية، ضمن برنامج سري واسع».
Washington Post,
http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html
15. ديفيد جلبرت (4 يوليو 2013). مجلة إنترناشيونال بيزنس تايمس. مقال: «بعد الكشوفات عن تجسس وكالة الأمن القومي»، الشركات تتجه إلى سويسرا لتخزين بيانات «حوسبة السحاب».
International Business Times,
<http://www.ibtimes.co.uk/business-turns-away-dropbox-towards-switzerland-nsa-486613>.
16. إلين ميسمر (8 يناير 2014). مقال: «فضيحة وكالة الأمن القومي» تطارد شركات المعلوماتية والاتصالات في بريطانيا وكندا.
<http://www.networkworld.com/article/2173190/security/nsa-scandal-spooking-it-pros-in-uk-canada.html>.
17. شركة إن تي تي كوميونيكايشنز (28 مارس 2014). تقرير: «صدمات ما بعد وكالة الأمن القومي»: سونون غير مقارنة صنّاع القرار في شركات المعلوماتية والاتصالات، لموضوع «حوسبة السحاب».
http://nsaaftershocks.com/wp-content/themes/nsa/images/NTTC_Report_WEB.pdf
18. دانيال كاسترو (5 أغسطس 2013). «مؤسسة الابتكار وتقنية المعلومات». دراسة: «كم يكلف برنامج «بريزم» شركات «حوسبة السحاب» الأمريكية؟»
Information Technology and Innovation Foundation,
<http://www.itif.org/publications/how-much-will-prism-cost-us-cloud-computing-industry>
- أندريا بيترسون (7 أغسطس 2013). صحيفة واشنطن بوست. مقال: «تجسس وكالة الأمن القومي» يكلف شركات التكنولوجيا الأمريكية 35 بليون دولار في 3 سنوات.
Washington Post,
<http://www.washingtonpost.com/blogs/the-switch/wp/2013/08/07/nsa-snooping-could-cost-us-tech-companies-35-billion-over-three-years>.
19. جيمس ستاتن (14 أغسطس 2013). «مدونة إلكترونية». مقال: «خسائر برنامج «بريزم» ستفوق التوقعات المتأولة».
James Staten's Blog,
http://blogs.forrester.com/james_staten/13-08-14-the_cost_of_prism_will_be_larger_than_itif_projects
20. كريستوفر ميامز (14 نوفمبر 2013). مقال: «خسائر «سيسكو» الفصلية الموجهة توضح أن تجسس وكالة الأمن القومي» يمكنه أن يبعد الشركات الأمريكية عن سوق بقرابة تريليون دولار».
<http://qz.com/147313/ciscos-disastrous-quarter-shows-how-nsa-spying-could-freeze-us-companies-out-of-a-trillion-dollar-opportunity>
21. أنطون توديانوفسكي وتوماس غريتا وسام شوشنر (30 أكتوبر 2013). صحيفة وول ستريت جورنال. مقال: «فضيحة وكالة الأمن القومي» تخنق شركة «إيه تي أند تي».

Wall Street Journal,

<http://online.wsj.com/news/articles/SB10001424052702304073204579167873091999730>

22. وولف ريشتر (17 أكتوبر 2013). مقال: «الكشوفات عن وكالة الأمن القومي» تقتل المبيعات الإلكترونية لشركة «آي بي إم» في الصين.

<http://www.testosteronepit.com/home/2013/10/17/nsa-revelations-kill-ibm-hardware-sales-in-china.html>

23. سبنسر ي. أنتي (22 نوفمبر 2013). صحيفة وول ستريت جورنال. مقال: «مدير «كوالكوم» يورد أن فضيحة «وكالة الأمن القومي» تؤثر في أعمال شركته في الصين».

Wall Street Journal,

<http://online.wsj.com/news/articles/SB10001424052702304337404579214353783842062>

24. مارك سكوت (26 يونيو 2014). صحيفة نيويورك تايمس. مقال: «متأثرة بفضيحة «وكالة الأمن القومي»، ألمانيا تلغي عقداً ضخماً مع «فيريزون» الأمريكية».

New York Times,

<http://www.nytimes.com/2014/06/27/business/angered-by-nsa-activities-germany-cancels-verizon-contract.html>

25. ستيفن كارتر (13 فبراير 2014). شبكة «بلومبرغ نيوز» التلفزيونية. مقال: «فجوة الثقة المكلفة للشركات الأمريكية».

Bloomberg BusinessWeek,

<http://www.businessweek.com/articles/2014-02-13/nsasnooping-backlash-could-cost-u-dot-s-dot-tech-companies-billions>

كلير كاين ميلر (22 مارس 2014). صحيفة نيويورك تايمس. مقال: «تجسس «وكالة الأمن القومي» يلقي بتكاليف ضخمة على شركات المعلوماتية الأمريكية».

New York Times,

<http://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurtingbottom-line-of-tech-companies.html>

26. أشلي لو (18 مايو 2014). وكالة «رويترز» للأنباء. مقال: «جون تشامبرز يحض إدارة أوباما على كبح تجسس «وكالة الأمن القومي»».

Reuters,

<http://www.reuters.com/article/2014/05/18/cisco-systems-nsa-idUSL1N0040F420140518>

27. شون كالامار (14 مايو 2014). موقع «آرس تكنيكا». مقال: «صور مصنع «الترقية» لـ«وكالة الأمن القومي» تظهر زرع مكونات في محولات شركة «سيسكو»».

<http://arstechnica.com/tech-policy/2014/05/photos-of-an-nsa-upgrade-factory-show-ciscorouter-getting-implant>

28. دومينيك روش (11 سبتمبر 2013). صحيفة «الغارديان». مقال: «زوكربيرغ يعتبر أن الحكومة الأمريكية «حطمت الأمور» بتصرّياتها عن «وكالة الأمن القومي»».

Guardian,

<http://www.theguardian.com/technology/2013/sep/11/yahoo-ceo-mayer-jail-nsa-surveillance>

29. كورنيليس رامن (13 سبتمبر 2011). تلفزيون «بلومبرغ». مقال: «تطلب «دويتشه تليكوم» صنع «سحابة ألمانية» لتبقي بياناتها بعيداً عن الولايات المتحدة».

Bloomberg News,

<http://www.bloomberg.com/news/2011-09-13/deutsche-telekom-wants-german-cloud-toshield-data-from-u-s-.html>

30. آليسون غراند (20 نوفمبر 2013). مقال: «وفق المحاكم، تنتهك سياسات «غوغل» قوانين ألمانيا في الخصوصية».
<http://www.law360.com/articles/490316/google-s-policies-violate-german-privacy-law-court-says>
31. لويك إيسر (18 فبراير 2014). مقال: «وفق المحاكم، يجب على «فيسبوك» الانصياع لقوانين ألمانيا في حماية البيانات».
<http://www.pcworld.com/article/2098720/facebook-must-comply-with-german-data-protection-law-court-rules.html>
32. لويك إيسر (7 مايو 2013). مقال: «وفق المحاكم، تتعارض قواعد «أبل» في الخصوصية مع قوانين ألمانيا في حماية البيانات».
<http://www.macworld.com/article/2038070/apples-privacy-policy-violates-german-data-protection-law-berlin-court-rules.html>
33. صحيفة دير شبيغل (5 أغسطس 2013). مقال: «ارتدادات فضيحة «وكالة الأمن القومي»: وزير ألماني يروج لحظر الشركات الأمريكية».
Der Spiegel,
<http://www.spiegel.de/international/business/german-minister-on-eu-company-ban-for-privacy-violation-a-914824.html>
34. كريستا هاغز (27 مارس 2014). وكالة «رويترز». مقال: «خصوصية البيانات ترسم الجيل الجديد من حواجز التجارة الدولية».
Reuters,
<http://www.reuters.com/article/2014/03/27/us-usa-trade-tech-analysis-idUSBREA2Q1K120140327>
35. يعلق مديرون لشركات أمريكية من ممارسة الحمائية ضد شركائهم. ستيفن لاسون (8 أكتوبر 2014). مقال: «تحذير من مديرين تنفيذيين: النفور من الرقابة الأمريكية يمكنه تحطيم الإنترنت».
<http://www.itworld.com/security/440886/jitters-over-us-surveillance-could-break-internet-tech-leaders-warn>
36. جيور ماسكولو وبين سكوت (أكتوبر 2013). مقال: «دروس من صيف سنودن: الطريق الصعب لاستعادة الثقة».
<http://www.newamerica.net/sites/newamerica.net/files/policydocs/NAF-OTI-WC-SummerOfSnowdenPaper.pdf>
- مارك سكوت (11 يونيو 2014). صحيفة نيويورك تايمز. مقال: «شركات أوروبية تجعل الخصوصية أداة ترويج لبيعاتها».
New York Times,
<http://bits.blogs.nytimes.com/2014/06/11/european-firms-turn-privacy-into-sales-pitch>
37. تمنح شركة «بروتون مابل» السويسرية بريدًا إلكترونيًا لا تطاله يد «وكالة الأمن القومي». جون بيفز (23 يونيو 2014). مقال: «شركة «بروتون مابل» السويسرية تقدم خدمة بريد إلكتروني لا شيء إلى «وكالة الأمن القومي»».
<http://techcrunch.com/2014/06/23/protonmail-is-a-swiss-secure-mail-provider-that-wont-give-you-up-to-the-nsa>
38. جونathan بالمار وجوزيف بايلي وسامر فرج (مارس 2000). دراسة: «دور الوسطاء في تطوير الثقة على الإنترنت: صعود الأطراف الثالثة الموثوقة ونصوص الخصوصية».
<http://onlinelibrary.wiley.com/doi/10.1111/j.1083-6101.2000.tb00342.x/full>
39. يانيس تزي وأخرون (يونيو 2007). دراسة: «تأثير الخصوصية الإلكترونية في سلوكيات التسوق: دراسة تجريبية».
<http://weis2007.econinfosec.org/papers/57.pdf>

40. كادي تومبسون (7 مارس 2014). شبكة «آن بي سي نيوز». مقال: «أترغب في الخصوصية على الإنترنت؟ الشركات الجديدة تراهن أن المستخدمين مستعدون للدفع».

NBC News,

<http://www.nbcnews.com/tech/security/want-privacy-online-start-ups-bet-users-are-ready-pay-n47186>

41. «داك داك غو».

<http://www.duckduckgo.com>.

42. شارون بروفيس (26 سبتمبر 2014). موقع «سي نت». مقال: «10 أشياء يجب أن تعرفها عن «إيللو»: الشبكة الاجتماعية الخالية من الإعلانات».

CNET,

<http://www.cnet.com/how-to/what-is-ello-thead-free-social-network>.

الفصل 10: الخصوصية

1. في ما يلي مقال يرجع إلى العام 1979، يتحدث عن الخصوصية كوسيلة لإخفاء الشخص حقائق عنه توجهاً لتضخيم سمعته. ريتشارد يوزنر (1979). مقال: «الخصوصية، السرية والسمعة».

http://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=2832&context=journal_articles

2. دأب دانيال سولوف على التصدي لمقولة «لا شيء لإخفائه». دانيال ج. سولوف (نوفمبر / ديسمبر 2007). مقال: «ليس لدي ما أخفيه»، والمفاهيم المغلوطة الأخرى عن الخصوصية».

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=998565

دانيال ج. سولوف (15 مايو 2011). مقال: «لماذا الخصوصية تكون مهمة حتى لو لم يكن لديك ما تخفيه».

3. صحيفة هافنغتون بوست (25 مايو 2011). مقال: «المدير التنفيذي لـ«غوغل» إريك شميدت يقول: إذا كان لديك ما لا تريد أي شخص آخر أن يعرفه، فلربما يجب عليك في المقام الأول ألا تفعل ذلك».

Huffington Post,

http://www.huffingtonpost.com/2009/12/07/google-ceo-on-privacy-if_n_383105.html

4. إلينور سميث (14 يوليو 2005). مقال: ««غوغل» يوازن بين الخصوصية والذئوع».

http://news.cnet.com/Google-balances-privacy,-reach/2100-1032_3-5787483.html.

راندال ستروس (28 أغسطس 2005). صحيفة نيويورك تايمس. مقال: «البحث عن أي شيء على «غوغل»، طالما أنه ليس «غوغل» نفسه».

New York Times,

<http://www.nytimes.com/2005/08/28/technology/28digi.html>

5. بوبي جونسون (10 يناير 2010). صحيفة الغارديان. مقال: «الخصوصية لم تعد عرفاً اجتماعياً، وفق مؤسس «فيسبوك»».

Guardian,

<http://www.theguardian.com/technology/2010/jan/11/facebook-privacy>

6. برايان بايلي (11 أكتوبر 2013). مقال: «زوكربيرغ يشتري أربعة منازل قرب مسكنه في «بالو ألتو»».

http://www.mercurynews.com/business/ci_24285169/mark-zuckerberg-buys-four-houses-near-his-palo-altohome.

7. بيتري. ساند (ربيع / صيف 2006). مقال: «قيمة الخصوصية».

<http://moritzlaw.osu.edu/students/groups/is/files/2012/02/5-Sand.pdf>.

8. جوديث دوناث (2014). «مطبعة معهد ماساشوستس للتقنية». كتاب: الآلة الاجتماعية: تصاميم من أجل العيش على الإنترنت.
MIT Press,
<https://encrypted.google.com?id=XcgmwEACAAJ>
9. ديفيد كيركاتريك (2010). «دار سايمون أند شوستر». كتاب: تأثير «فيسبوك»: القصة الداخلية للشركة التي تربط العالم.
<https://www.facebook.com/thefacebookeffect>
10. يعرف إيبين موغلن الخصوصية في ثلاثة مكونات: «الأول هو السرية بمعنى قدرتنا على الحفاظ على محتوى رسائلنا فلا يعرفها سوى من نقصد إرسالها لهم. الثاني هو إغفال الهوية بمعنى سرية من يرسل الرسائل ومن يتلقاها، عندما يتعذر الحفاظ على محتوى الرسائل. من الأهمية بمكان أن نحظى بإمكان إغفال الهوية في ما ننشره ونقرأه. الثالث هو الاستقلالية الذاتية، بمعنى قدرتنا على اتخاذ القرارات المتعلقة بحياتنا، بعيداً عن أي قوة تسعى لانتهاك سريتنا أو إغفالنا الهوية». إيبين موغلن (27 مايو 2014)، صحيفة الغارديان. مقال: «الخصوصية تتعرض للهجوم: وثائق وكالة الأمن القومي» تكشف تهديدات جديدة للديمقراطية.
Guardian,
<http://www.theguardian.com/technology/2014/may/27/-sp-privacy-under-attack-nsa-files-revealed-new-threats-democracy>.
ويقسم دانيال ج. سولوف أستاذ القانون في «جامعة جورج واشنطن» الخصوصية إلى 6 أقسام: «1- الحق في أن نترك لأشأننا. 2- تقييد وصول الآخرين إلى ذاتنا. 3- السرية. 4- السيطرة على المعلومات الشخصية. 5- امتلاك النفس. و6- الحميية».
- Daniel J. Solove (Jul 2002), «Conceptualizing privacy», *California Law Review* 90,
<http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1408&context=california-law-review>
11. دانا بويد (2014). «مطبعة جامعة يال». كتاب: معقدة: الحياة الاجتماعية للمراهقين المتصلين شبكياً.
<http://www.danah.org/books/ItsComplicated.pdf>.
12. اختبرت تلك اليوتوبيا المعكوسة في الأدب وأخيلته. دايف إيفرز (2013). رواية: الدائرة.
<http://www.mcsweeneys.net/articles/a-brief-q-a-with-dave-eggers-about-his-new-novel-the-circle>
13. هيلين نسينباوم (خريف 2011). دراسة: «مقاربة سياقية للخصوصية على الإنترنت».
http://www.amacad.org/publications/daedalus/11_fall_nissenbaum.pdf
آليكس مادريغال (29 مارس 2012). مجلة أتلانتيك. مقال: «الفيلسوف الذي ترك بصماته على السياسة الجديدة للجنة التجارة الفيدرالية، بشأن الخصوصية».
- Atlantic,
<http://www.theatlantic.com/technology/print/2012/03/the-philosopher-whose-fingerprints-are-all-over-the-ftcs-new-approach-to-privacy/254365>.
14. جورج بنيشاس (مايو 2014). بحث: «نظرية الانتهاك في الخصوصية».
<http://link.springer.com/article/10.1007%2Fs11158-014-9240-3>
15. بيتر كلويفر ودانيال روبنشتاين (صيف 1977). بحث: «مفهوم الخصوصية وأساسه البيولوجية».
https://www.princeton.edu/~dir/pdf_dir/1977_Klopper_Rubenstein_JSocIssues.pdf.
16. بيتر واتس (9 مايو 2014). بحث: «مجتمع الأرض المحروقة: دليل المفجر الانتحاري إلى الخصوصية على الإنترنت».
<http://www.rifters.com/real/shorts/TheScorchedEarthSociety-transcript.pdf>.
17. سيدني جورار (ربيع 1966). بحث: «عن المناحي النفسية للخصوصية».
<http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=3110&context=lcp>.
18. جيمس وتمان (أبريل 2004). مقال: «نظرتان ثقافتان غربيّتان إلى الخصوصية: الكرامة في مواجهة الحرية».
<http://www.yalelawjournal.org/article/the-two-western-cultures-of-privacy-dignity-versus-liberty>.

19. مايكل لينش (22 أكتوبر 2013). صحيفة نيويورك تايمس. مقال: «الخصوصية وتهديد الذات».
<http://opinionator.blogs.nytimes.com/2013/06/22/privacy-and-the-threat-to-the-self>.
20. صودرت تلك الوثائق في سياق قضية «إيران- كوتراس». مايكل تاكيت (14 شباط 1987). صحيفة شيكاغو تريبيون. مقال: «سجلات الكمبيوتر تروي حكايات إيران: مواد مطبوعة بواسطة الكمبيوتر تدل المفتشين على مذكرات من رسميين».
- Chicago Tribune*,
http://articles.chicagotribune.com/1987-02-14/news/8701120148_1_nsc-staff-professional-office-system-profs
21. إليزابيث وازرمان (17 نوفمبر 1998). شبكة «سي أن أن». مقال: «محفوظات غيتس تثير ضحك القضاة».
 CNN,
<http://edition.cnn.com/TECH/computing/9811/17/judgelaugh.ms.idg>.
22. بيل متهنسون (31 أغسطس 2014). صحيفة نيويورك دايلي نيوز. مقال: «جينيفر لورانس وممثلات أخريات، تسربت صورهن عاريات بعد فضيحة تسرب بيانات ضخمة».
- New York Daily News*,
<http://www.nydailynews.com/entertainment/gossip/jennifer-lawrence-celebrities-nude-photos-leaked-internet-article-1.1923369>
23. للغاية نفسها، تسوق شركة «سيرفال بيومتركس» ماسحات ضوئية لرخص قيادة المركبات. شركة «سيرفال بيومتركس» (2014). منشور: «أمن النوادي: ماسحات ضوئية لبطاقات الهوية مخصصة للبارات والنوادي الليلية».
- <http://www.servallbiometrics.com/index.php/products>
24. (14 مايو 2007). مقال: «رسم المستقبل»، في مدونة «تشارلي دايري»، الإلكترونية.
Charlie's Diary,
http://www.antipope.org/charlie/blog-static/2007/05/shaping_the_future.html.
25. هناك مقال قصير لتيد شيانغ يعالج ذلك الأمر، عنوانه «حقيقة الواقع، حقيقة الشاعر».
http://subterraneanpress.com/magazine/fall_2013/the_truth_of_fact_the_truth_of_feeling_by_ted_chiang.
26. كان الباحث في الاتصالات هارولد ايننيس سباقاً في وصف الافتراضات القبلية الموجودة في أشكال الاتصالات المختلفة. ولاحظ أن بعض وسائل الاتصالات تحفظ الاتصال بالوقت، فيما تعمل وسائل أخرى بواسطة الأمكنة. هارولد ايننيس (1951)، كتاب: الافتراض القبلي في الاتصال. «مطبعة جامعة تورنتو».
<http://books.google.com?id=egwZyS26booC>
27. هناك بحوث أخانة في هذا الشأن. نحن ننسى تفاصيل حوادث مهمة أيضاً. إذ درس بحثة ذكريات الناس عن أمكنة وجودهم أثناء مشاهدتهم انفجار مكوك الفضاء «تشالنجر»، والإعلان عن نتيجة محاكمة لاعب البيسبول الأسمر أو. جي. سيمبسون بقضية مقتل عشيقته، وتغطية ضربات الإرهاب في 9/11. جون نيل بوحنون الثالث (يوليو 1998)، مقال: «التماعات الذاكرة في تدكر كارثة مكوك الفضاء: قصة نظريتين».
<http://www.sciencedirect.com/science/article/pii/S0010027788900364>
- أندرو آر. إيه. كونواي وآخرون (يوليو 2008). «التماعات الذاكرة عن حوادث 11/9».
<http://onlinelibrary.wiley.com/doi/10.1002/acp.1497/abstract>
28. متشيل ناتيفيداد رودريغز وموريس إمسيليم (مارس 2011). «مشروع القانون القومي للتوظيف». بحث: «65 مليوناً يجب ألا يتقدموا للوظائف: نظرة إلى إعادة رسم الخلفية الجرمية للمتقدمين للوظائف».
 National Employment Law Project,
http://www.nelp.org/page/-/65_Million_Need_Not_Apply.pdf.
29. ويندي هيو كيونغ شون (خريف 2008). مقال: «الزائل الصامد، أو الذاكرة هي المستقبل».
<http://www.ucl.ac.uk/art-history/events/past-imperfect/chun-reading>
30. بروس شنابر (27 فبراير 2014). صحيفة الغارديان. مقال: «الروبوتات الافتراضية لـوكالة الأمن القومي، تعمل على «جمع» بياناتك، ولا يحاسبها أحد على ذلك».

Guardian,

<http://www.theguardian.com/commentisfree/2014/feb/27/nsa-robots-algorithm-surveillance-bruce-schneier>

31. «مؤسسة الحدود الإلكترونية» (2013). وثيقة: «تلاعب الحكومة بالكلمات عند الحديث عن التجسس المحلي لدوكالة الأمن القومي».

<https://www.eff.org/nsa-spying/wordgames>

تيم تريفور (14 أغسطس 2013). «مؤسسة الحدود الإلكترونية». بحث: «دليل إلى الخداع والتضليل والتلاعب بالكلمات، الذي يلجأ إليه الرسمىون لتضليل الجمهور عند حديثهم عن رقابة «وكالة الأمن القومي»».

Electronic Frontier Foundation,

<https://www.eff.org/deeplinks/2013/08/guide-deceptions-word-games-obfuscations-officials-use-mislead-public-about-nsa>

32. أورد دليل عن المهمات صادر في 1982، أنه: «... يجب أن يستخدم وصف «جمع» للمعلومات حصرياً عندما يجري تلقّيها من موظف في القسم الاستخباراتي من «وزارة الدفاع» بهدف الاستعمال، في سياق مهماته الرسمية». وكذلك: «يستعمل وصف «جمع» للمعلومات التي تصل من الوسائط الإلكترونية، بصورة حصريّة عند تحويلها إلى شكل قابل للفهم». وزارة الدفاع الأميركية، مكتب نائب وزير الدفاع (ديسمبر 1982). فصل: «الإجراءات التي تتحكم بنشاطات الأقسام الاستخباراتية في وزارة الدفاع، عندما تكون مؤثرة في الأشخاص في الولايات المتحدة».

DoD 5240-1R, p. 15,

http://www.fas.org/irp/doddir/dod/d5240_1_r.pdf.

33. تبدي وزارة الدفاع تحوّلات حتى ضد مجرد التفكير بالكلمات واستعمالها بشكل صحيح. «الإجراء 2 يقود قارئ المذكرة» 5204.1 - آر، أثناء تعرّفه للمزّة الأولى إلى «متاهة» القوانين. للبدء بالرحلة، من الضروري التوقّف أولاً وضبط الألفاظ التي تستعملها. إن الكلمات والمصطلحات الواردة في المذكرة - 5204.1 آر لها معانٍ محدّدة، ويحدث غالباً أن ينقاد البعض بعيداً عندما يعتمدون على المعنى الشائع أو المفهومي، لتعريف كلمة معينة».

US Defense Intelligence Agency, Defense HUMINT Service (Aug 2004), *Intelligence Law Handbook*, Defense Intelligence Management Document CC-0000-181-95,

<https://www.aclu.org/files/assets/eo12333/DIA/Intelligence%20Law%20Handbook%20Defense%20HUMINT%20Service.pdf>.

34. أندريا ميتشيل (9 يونيو 2013). شبكة تلفزيون «أن بي سي». مقال: «مقطّفات من مقابلة أندريا ميتشيل مع جيمس كلايبر، مدير الاستخبارات القومية».

NBC News,

<http://www.nbcumv.com/mediavillage/networks/nbcnews/pressreleases?pr=contents/pressreleases/2013/06/09/nbcnewsexclusiv1370799482417.xml>.

35. رون وايدن (12 مارس 2013). موقع «يوتيوب». «وايدن في جلسة الاستماع للاستخبارات عن الرقابة بالدجي بي أس» وجمع «وكالة الأمن القومي» البيانات».

YouTube,

<https://www.youtube.com/watch?v=QwiUVUJmGjs>.

36. «غوغل» (2014). «الإعلانات في «جي ميل»».

<https://support.google.com/mail/answer/6603?hl=en>

37. في 2010، طمأنتنا «وكالة أمن النقل» بأن أجهزة المسح الضوئي للجسد كاملاً، لا تخزّن معلومات. في ما بينت ووافق سُلّمت إلى «مركز معلومات الخصوصية الإلكترونية» أن تلك المساحات تُشخّن مع أقراص صلبة ومنافذ لأدوات ذاكرة الفلاش من نوع «يو إس بي». غينغر ماككول (3 أغسطس 2010). تقرير: «وثائق تظهر أن مساحات الأجساد ضوئياً تخزن البيانات روتينياً».

Electronic Privacy Information Center,

http://epic.org/press/EPIC_Body_Scanner_Press_Release_08_03_10.pdf.

Declan McCullagh (4 Aug 2010), «Feds admit storing checkpoint body scan images», *CNET*,

<http://www.cnet.com/news/feds-admit-storing-checkpoint-body-scan-images>.

إدارة وكالة أمن النقل، (6 أغسطس 2010). «المُدونة الإلكترونية للوكالة». «رد وكالة أمن النقل» على أسئلة السلطة الفيدرالية، يعترف بأن نقاط التفتيش تخزن صوراً ضوئية للأجساد.

TSA Blog,

<http://blog.tsa.gov/2010/08/tsa-response-to-feds-admit-storing.html>

38. للسبب عينه، لا نحتاج على الدمى من نوع «فوربيز»، لكننا قد نحتاج لو أنها تحتوي أدوات تسجيل. ومع ذلك، أبدت «وكالة الأمن القومي» قلقها لبعض الوقت؛ بشأن ذلك الأمر. «هيئة الإذاعة البريطانية» (13 يناير 1999). «هل «فوربي» دمية أم جاسوس»؟

BBC News,

<http://news.bbc.co.uk/2/hi/americas/254094.stm>.

39. بروس شنابر (21 أكتوبر 2013). مجلة أتلانتيك. مقال: «ليس منطقياً دفاع وكالة الأمن القومي» عن الجمع المكثف للبيانات».

Atlantic,

<http://www.theatlantic.com/politics/archive/2013/10/why-the-nsas-defense-of-mass-data-collection-makes-nonsense/280715>.

40. بروس شنابر (2000). كتاب أسرار وأكاذيب. دار «ويلي» للنشر.

<http://www.wiley.com/WileyCDA/WileyTitle/productCd-0471453803.html>.

41. تشارلز غلاسر (1 يونيو 2011). «جامعة جورج واشنطن». دراسة: «ردع الهجمات السبرانية والأمن الاستراتيجي للولايات المتحدة».

Report GW-CSPRI-2011-5, George Washington University Cyber Security Policy and Research Institute,

http://www.cspri.seas.gwu.edu/uploads/2/1/3/2/21324690/2011-5_cyber_deterrence_and_security_glaser.pdf.

جوزيف س. ناي (يونيو 2010). «كلية كينيدي في جامعة هارفرد». دراسة: «قوة الفضاء السبراني».

Harvard Kennedy School, Belfer Center for Science and International Affairs,

<http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf>.

42. تشارلز كلوفر (11 مارس 2009). صحيفة فايننشال تايمس. مقال: «مجموعة يساندها الكرملين مسؤولة عن الهجمات السبرانية على أستراليا».

Financial Times,

<http://www.ft.com/cms/s/0/57536d5a-0ddc-11de-8ea3-0000779fd2ac.html>

43. نيكول بيرلر (31 يناير 2013). صحيفة نيويورك تايمس. مقال: «مجموعة «هاكرز» من الصين هاجمت نيويورك تايمس خلال الشهر الماضي».

New York Times,

<http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html>.

44. ويليام جي. برود، جون ماركوف وديفيد ي. سانغر (15 يناير 2011). صحيفة نيويورك تايمس. مقال: «تجربة إسرائيلية على دودة إلكترونية أتت لتأخير في برنامج إيران النووي».

New York Times,

<http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html>

ديفيد ي. سانغر (1 يونيو 2012). صحيفة نيويورك تايمس. مقال: «أوباما أمر بشن سلسلة غارات سبرانية ضد إيران».

New York Times,

<http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html>.

45. تقييد إغفال الهوية لا يقضي على التصييد. إذ إن سلوك الناس على الإنترنت معقد، وهو أقرب إلى إرخاء القيود الاجتماعية منه إلى السعي لإغفال الهوية. جون سولر (يونيو 2004). مقال: «التحلل الاجتماعي في الفضاء الافتراضي».

<http://online.liebertpub.com/doi/abs/10.1089/1094931041291295>.

46. فيليب وينتر وستيفان ليندسكوك (6 أغسطس 2012). «منتدى «يونيكس». ورقة بحث: «كيف يعمل جدار النار» الصيني العظيم على صد نظام «تور»».

USENIX Workshop on Free and Open Communications on the Internet, Bellevue, Washington, <https://www.usenix.org/system/files/conference/foci12/foci12-final2.pdf>

47. ليون بانيتا (11 أكتوبر 2012). وزارة الدفاع. «ملاحظات من وزير الدفاع ليون بانيتا حول الأمن السبراني، إلى المدراء التنفيذيين للشركات المهتمين بالأمن القومي».

US Department of Defense,

<http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136>.

الفصل 11: الأمن

1. بروس شنابير (17 مايو 2007). مجلة وايرد. مقال: «دروس من الهجوم في «جامعة فرجينيا»: المخاطر النادرة تولد ردود أفعال لا عقلانية».

Wired,

http://archive.wired.com/politics/security/commentary/securitymatters/2007/05/securitymatters_0517

2. المدونة الإلكترونية لواشنطن (15 أغسطس 2014). مقال: «أنت معرض للموت على يد شرطي بتسعة أضعاف موتك بيد إرهابي».

Washington's Blog,

<http://www.washingtonsblog.com/2014/08/youre-nine-times-likely-killed-police-officer-terrorist.html>

3. سينسر إكرمان (13 ديسمبر 2013). صحيفة الغارديان. مقال: «تقارير تفيد بأن «وكالة الأمن القومي» تفكر بعدم إحداث تغيير واسع في برامجها للتجسس».

Guardian,

<http://www.theguardian.com/world/2013/dec/13/nsa-review-to-leave-spying-programs-largely-unchanged-reports-say>.

4. عندما نسترجع حدثاً ما ونرى الأدلة كلها، نعتقد غالباً بأنه كان واجباً علينا توصيل النقط. يملك ذلك الأمر اسماً: التحيز بالاسترجاع. إذ تتوضح الأجزاء المفيدة من البيانات بعد الواقعة، أما قبلها فلم تكن تلك الأجزاء سوى قسم يسير من ملايين البيانات العديمة الدلالة. وكذلك فمن الممكن تجميع تلك الأجزاء نفسها لتدل على مليون اتجاه مختلف.

5. نيسم نيكولاس طالب (2007). «مغالطة السرد» في كتاب البجعة السوداء: تأثير غير متوقع تماماً. دار «راندوم هاوس».

<http://www.fooledbyrandomness.com>.

6. وكالة أنباء «أسوشيتدبرس» (2 فبراير 2012). صحيفة يو أس إيه توداي. مقال: «القائمة الأميركية للممنوعين من السفر جواً تتضاعف في سنة واحدة».

USA Today,

<http://usatoday30.usatoday.com/news/washington/story/2012-02-02/no-fly-list/52926968/1>.

7. إريك شميدت ومايكل س. شميدت (24 أبريل 2013). صحيفة نيويورك تايمس. «وكالتان أمريكيتان وضعتا مفجّر ماراثون «بوسطن» على قوائمهما للمراقبة».
New York Times,
<https://www.nytimes.com/2013/04/25/us/tamerlan-tsarnaev-bomb-suspect-was-on-watch-lists.html>
8. ي. دبليو. شي نفاي وآخرون (فبراير 2011). دراسة: «تطبيق تقنية التنقيب في البيانات في تقصي تزوير بطاقات الائتمان: إطار أكاديمي للعمل ومراجعة للأدبيات».
<https://www.sciencedirect.com/science/article/pii/S0167923610001302>
9. إيريسكا هاريل ولين لانغتون (12 ديسمبر 2013). مكتب الإحصاءات في وزارة العدل. تقرير: «ضحايا سرقة الهوية في 2012».
US Bureau of Justice Statistics,
<http://www.bjs.gov/index.cfm?ty=pbdetail&iid=4821>.
10. «مكتب الموثوقية الحكومية» (2013). تقرير: «التزوير الضارثي في الملاذات الآمنة: وكالة المداخل الداخلية»
تجمع بلايين الدولارات، لكن التزوير الضارثي مستمر».
Report GAO-13-318,
<http://www.gao.gov/assets/660/653369.pdf>
11. والتر بيرري وآخرون (2013). «مؤسسة راند». بحث: «شرطة توقعية: دور توقع الجرائم في عمليات إنفاذ القانون».
RAND Corporation,
<https://www.ncjrs.gov/pdffiles1/nij/grants/243830.pdf>.
12. جون مولر ومارك ستيوارت (2011). «مطبعة جامعة أوكسفورد». كتاب: إرهاب، أمن ونقود: التوازن بين المخاطر والفوائد والتكاليف في وزارة الأمن الوطني.
Oxford University Press, chap. 2,
<http://books.google.com/books?id=jyYGL2jZBC4C>
13. جيف جوناس وجيم هاربر (11 ديسمبر 2006). منشورات مؤسسة «كاتو». «الكفاءة في محاربة الإرهاب والدور المحدود للتنقيب التوقعي في البيانات».
Cato Institute,
<http://www.cato.org/publications/policy-analysis/effective-counterterrorism-limited-role-predictive-data-mining>.
14. فريد كايت (صيف 2008). جامعة هارفرد. دراسة: «التنقيب الحكومي في البيانات: الحاجة إلى إطار قانوني».
Harvard Civil Rights-Civil Liberties Law Review
43,
http://www.law.harvard.edu/students/orgs/crcl/vol43_2/435-490_Cate.pdf.
- ج. ستيوارت مندونهال ومارك شميدوهوفر (شتاء 2012-2013). دراسة: «اختبار انتقائي للإرهاب».
<http://object.cato.org/sites/cato.org/files/serials/files/regulation/2013/1/v35n4-4.pdf>
- كوربي شيفرز (6 يونيو 2013). مقال: «ما أرجحية أن يلتقط برنامج «بريزم» لوكالة الأمن القومي، إرهابيًا؟».
<http://bayesianbiologist.com/2013/06/06/how-likely-is-the-nsaprim-program-to-catch-a-terrorist>
- مارسي ويلر (15 يونيو 2013). مقال: «انعدام كفاءة «الأخ الكبير»: الروابط ومصنع الإرهاب».
<http://www.emptywheel.net/2013/06/15/the-inefficacy-of-big-brother-associations-and-the-terror-factory>.
15. في علم الإحصاء، يسمّى ذلك «مغالطة المعدّل الأساسي»، وينطبق على حقول أخرى. ومثلاً، حتى أشد الفحوص الطبية دقة تصبح أداة انتقاء مثيرة للإشكاليات، عندما تكون نسبة المرض نادرة بين السكان. وتعمّدت ألا أناقش الرياضيات التي تكمن خلف ذلك، لكن المهتمين يستطيعون قراءة تلك التفاصيل. جيف جوناس وجيم

هاربر (11 ديسمبر 2006). منشورات مؤسسة «كاتو». «الكفاءة في محاربة الإرهاب والدور المحدود للتنقيب التوقفي في البيانات».

Cato Institute,

<http://www.cato.org/publications/policy-analysis/effective-counterterrorism-limited-role-predictive-data-mining>

16. ج.د. توسيل (19 يونيو 2013). مقال: «لماذا تتجسس على الجميع؟ لأنك تحتاج كومة القش كي تمثر على الإبرة».

Reason,

<http://reason.com/blog/2013/07/19/why-spy-on-everybody-because-you-need-th>

17. مايك مازنيك (15 أكتوبر 2013). موقع «تيك درت». مقال: «الوثائق الأخيرة عن «وكالة الأمن القومي» تظهر أن الإفراط في «تجميع القش» يصعب عمل الوكالة».

Tech Dirt,

<https://www.techdirt.com/articles/20131014/17303424880/latest-revelationsshow-how-collecting-all-haystacks-to-find-data-makes-nsas-job-harder.shtml>

18. كريس يونغ (12 مارس 2012). مجلة فوربس. مقال: «إعادة تعريف الاستخبارات العسكرية: البيانات الضخمة في أرض المعركة».

Forbes,

<http://www.forbes.com/sites/techonomy/2012/03/12/military-intelligence-redefined-big-data-in-the-battlefield>

برنامج «وكالة الأمن القومي» في التجسس. مات بريغز (7 يونيو 2013). مدونة «مات بريغز». مقال: «التنقيب في البيانات: «بريزم»، «وكالة الأمن القومي» والإنذارات الكاذبة الإيجابية: تحديث».

William M. Briggs,

<http://wmbriggs.com/blog/?p=8239>

19. لويل بيرغمان وآخرون (17 يناير 2006). صحيفة نيويورك تايمز. مقال: «بيانات وكالة تجسس بعد 11/9، أوصلت الداف بي أي» إلى طرق مسدودة».

New York Times,

<http://www.nytimes.com/2006/01/17/politics/17spy.html>.

20. «مكتب الموثوقية الحكومية» (26 مارس 2013). تقرير: «المشاركة في المعلومات: خطوات إضافية مطلوبة لتدعيم المشاركة في التقارير عن النشاطات المشبوهة المتصلة بالإرهاب».

Report GAO-13-233,

<http://www.gao.gov/assets/660/652995.pdf>.

21. يوشاي بنكلر (8 أكتوبر 2013). صحيفة الغارديان. مقال: «حقيقة: لا تحصل «وكالة الأمن القومي» إلا معلومات شحيحة من «ميتاداتا» الأميركيين. لذا، فلتتوقف عن جمعها».

Guardian,

<http://www.theguardian.com/commentisfree/2013/oct/08/nsa-bulk-metadata-surveillance-intelligence>.

بيتر برغن (يناير 2014). مقال: «هل توقف برامج التجسس المكثفة لـ «وكالة الأمن القومي» الإرهاب؟»

http://newamerica.net/publications/policy/do_nsa_bulk_surveillance_programs_stop_terrorists

22. مارسي ويلر (12 ديسمبر 2013). مقال: «هل قاضت وزارة العدل بسالي موالين لجرد القول بنجاح «الفصل 15»؟»

<http://www.emptywheel.net/2013/12/12/did-doj-prosecute-basaaly-moalin-just-to-have-a-section-215-success>

23. يقدّم أمن الطائرات أمثلة كثيرة. في 2001، وضع ريتشارد رييد قنبلة في حذائه، وكان الأمر المباشر لذلك أنه يجب علينا جميعاً خلق أحيديتنا في المطارات منذها.

24. فرانسيس غويار (10 يونيو 2013). مجلة فورتشن. مقال: «لا تمثل البيانات الضخمة المتأنيّة من تجسّس وكالة الأمن القومي» حتى استراتيجية مجدية.

Fortune,

<http://management.fortune.cnn.com/2013/06/10/bigdata-nsa-spying-is-not-even-an-effective-strategy>

إد بلكينغتون ونيكولاس واط. (12 يونيو 2013). صحيفة الغارديان. مقال: «وفق خبراء، رقابة وكالة الأمن القومي» لم تقصد سوى خطط إرهابية قليلة تماماً.

Guardian,

<http://www.theguardian.com/world/2013/jun/12/nsa-surveillance-dataterror-attack>

25. جيفري سايفرت (3 أبريل 2008). خدمة الكونغرس للبحوث. تقرير: «التنقيب في البيانات والأمن الوطني»: مراجعة عامة.

Congressional Research Service,

<http://www.fas.org/sgp/crs/homesecc/RL31798.pdf>

26. بيتر بيرغن (30 ديسمبر 2013). شبكة «سي أن أن». مقال: «هل كان لرقابة وكالة الأمن القومي» كشف مخططات 9/11؟

CNN,

<http://www.cnn.com/2013/12/30/opinion/bergen-nsa-surveillance-september-11>

27. سايمون شوستر (19 أبريل 2013). مجلة تايم. مقال: «الإخوة تسارنايف: تلميحات إلى دوافع مفجّري «بوسطن»».

Time,

<http://world.time.com/2013/04/19/the-brothers-tsarnaevs-motives>.

28. مارسى ويلر (12 أبريل 2014). مقال: «بعد يوم من وضع كاتالوغات حكومية من البيانات التي جمعتها وكالة الأمن القومي»، رفضت وزارة العدل إصدار مذكرة إلى دزوخار [أحد مفجّري «بوسطن»].

<http://www.emptywheel.net/2014/04/12/the-day-after-governmentcatalogs-data-nsa-collected-on-tsarnaevs-doj-refuses-to-give-dzhokhar-notice>

29. «اللجنة القومية عن هجمات الإرهاب» (2004). «تقرير لجنة 11/9: التقرير النهائي لـ اللجنة القومية عن النشاطات الإرهابية ضد الولايات المتحدة».

<http://www.gpo.gov/fdsys/pkg/GPO-911REPORT/pdf/GPO-911REPORT.pdf>.

30. دان إيفين وكارين دي يونغ وسبنسر س. هسو (27 ديسمبر 2009). صحيفة واشنطن بوست. مقال: «المشتبه فيه في حادثة الطائرة كان مدرجاً في قاعدة بيانات عن الإرهاب، عقب تحذير والده رسميين أميركيين».

Washington Post,

<http://www.washingtonpost.com/wp-dyn/content/article/2009/12/25/AR2009122501355.html>.

31. دومينيك كاسكياني (7 سبتمبر 2009). «بي بي سي نيوز». مقال: «مخطط المتفجّرات السائلة: ما الذي حدث؟».

BBC News,

http://news.bbc.co.uk/2/hi/uk_news/8242479.stm

32. تفاخرت «وكالة الأمن القومي» بإحرازها 54 نجاحاً في مواجهة الإرهاب، لكن الرقم لم يصمد أمام التدقيق. لم تكن غالبية تلك الحالات مخططات إرهابية، ومعظمها كان خارج الولايات المتحدة. جويستون إليوت وثيودوريك ميبار (11 سبتمبر 2013). موقع «بروبابليكا». مقال: «مزاعم بأن وكالة الأمن القومي» «أحبطت مخططات» تنتشر على الرغم من غياب الأدلة.

Pro Publica,

<http://www.propublica.org/article/claim-on-attacks-thwarted-by-nsa-spreads-despite-lack-of-evidence>.

33. كيفن ستروم وجون هوليوود (2010). وزارة الأمن الوطني. مقال: «التأسيس على التلميحات: تقييم النجاح

والإخفاق في تقصي مخططات الإرهاب في الولايات المتحدة.

Institute for Homeland Security Solutions,

http://sites.duke.edu/ihss/files/2011/12/Building_on_Clues_Strom.pdf

34. بروس شنابر (8 سبتمبر 2005). مجلة وايرد. مقال: «الإرهابيون لا يصنعون مخططاتهم اقتباساً من الأفلام». *Wired*,

<http://archive.wired.com/politics/security/commentary/securitymatters/2005/09/68789>

35. بروس شنابر (2012). كتاب: كذبة ومتمردون: تفعيل الثقة التي يحتاجها المجتمع لينمو. دار «ويلي» للنشر.

<http://www.wiley.com/WileyCDA/WileyTitle/productCd-1118143302.html>.

36. روس أندرسون (2 أكتوبر 2001). «جامعة كامبريدج». دراسة: «صعوبة أمن البيانات: مقارنة اقتصادية».

University of Cambridge Computer Laboratory,

<http://www.acsac.org/2001/papers/110>

ماثيو ميلر وجون بريكي غريغوري كونتي (29 نوفمبر 2012). صحيفة الحروب الصغيرة. مقال: «لماذا يخطئ حدسك على الأرجح بشأن الأسلحة السبرانية؟».

Small Wars Journal,

<http://smallwarsjournal.com/jrnl/art/why-your-intuitionabout-cyber-warfare-is-probably-wrong>.

37. بروس شنابر (19 نوفمبر 1999). موقع «إنفورمايشن سكيوريتي». مقال: «مرافعة لأجل البساطة: لا تستطيع حماية ما لا تفهمه».

Information Security,

<https://www.schneier.com/essay-018.html>

38. إدوارد توفت (2003). «منتدى إدوارد توفت». تقرير: «لماذا يصعب صنع برامج رقمية جيدة؟».

Edward Tufte Forum,

http://www.edwardtufte.com/bboard/qand-a-fetch-msg?msg_id=0000D8

جيمس كواك (8 أغسطس 2012). صحيفة أتلانتيك. مقال: «البرامج الرقمية تدير العالم: ألا يجدر بنا التوجس من ضعف غالبيتها؟».

Atlantic,

<http://www.theatlantic.com/business/archive/2012/08/software-runs-the-world-how-scaredshould-we-be-that-so-much-of-it-is-so-bad/260846>.

39. مايكل رايلي (13 مارس 2014). مجلة بلومبرغ بيزنيس ويك. مقال: «إنذارات مهمة، والاستيلاء على 40 مليون رقم لبطاقات ائتمان: كيف انفجرت مسألة «تارغت»؟».

Bloomberg Businessweek,

<http://www.businessweek.com/articles/2014-03-13/target-missed-alarms-inepic-hack-of-credit-card-data>.

40. إليزابيث هاريس (17 يناير 2014). صحيفة نيويورك تايمس. مقال: «ممر مربب إلى محافظ نقود زبائن «تارغت»».

New York Times,

<http://www.nytimes.com/2014/01/18/business/a-sneaky-path-into-target-customers-wallets.html>

41. إليزابيث هاريس (6 مايو 2014). صحيفة نيويورك تايمس. مقال: «اختراق «تارغت» يطيح برئيسها».

New York Times,

<http://www.nytimes.com/2014/05/06/business/target-chief-executive-resigns.html>

42. نيكول برلرولث (31 يناير 2013). صحيفة نيويورك تايمس. مقال: «مجموعة «هاكرز» من الصين هاجمت نيويورك تايمس خلال الشهور الـ الماضية».

New York Times,

<http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html>.

43. يتمثل هدفها حاضراً في الوصول إلى سرعات في الحوسبة تقاس بالـ«إكزا فلوب» [إكزا= بليون بليون، والـ«فلوب» تعبير يعني «عملية طافية» وهو وصف لتناقل المعلومات في ذاكرة الكمبيوتر]. ما يساوي كوينتيليون [= واحد وإلى جانبه 18 صفراً] عملية في الثانية. جيمس بامفورد (15 مارس 2012)، مجلة وايرد، مقال: «وكالة الأمن القومي تبني المركز الأضخم للتجسس في البلاد (راقب ما تقوله)».

Wired,

http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/all

44. بروس شنابر (4 أكتوبر 2013). صحيفة الغارديان. مقال: «الجهوم على برنامج «تور»: كيف استهدفت «وكالة الأمن القومي» إخفاء الهوية لمستخدمي الإنترنت».

Guardian,

<http://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity>

45. غلين غرينوالد وإدوارد سنودن (17 يوليو 2013). صحيفة الغارديان. مقال: «إدوارد سنودن، مُطلق صافرة الإنذار، يجيب عن أسئلة القراء».

Guardian,

<http://www.theguardian.com/world/2013/jun/17/edward-snowden-nsa-files-whistleblower>

46. هناك نقاش عن أخلاقيات ذلك الأمر في الموضوع التالي. سيرج إيغلمان وكورماك هيرلي وبول س. فان أورشوت (سبتمبر 2013)، ورقة بحث: «أسواق التوظيفات في «اليوم صفر»: الأخلاقيات والإملاءات».

<http://www.nspw.org/papers/2013/nspw2013-egelman.pdf>

47. ستيفن فراي (5 ديسمبر 2013). مقال: «المجهولون المعروفون: تحليل تجريبي عن ثغرات الأمن غير المعلنة». https://www.nsslabs.com/system/files/public-report/files/The%20Known%20Unknowns_1.pdf.

48. أندري غرينبرغ (21 مارس 2012). مجلة فوربس. مقال: «تعرف إلى «الهاكرز» الذين يبيعون للجواسيس أدوات تستطيع اختراق كمبيوترك (ويحصلون على أموال بستة أضعاف لقاء ذلك)».

<http://www.forbes.com/sites/andygreenberg/2012/03/21/meet-the-hackers-who-sell-spiethe-tools-to-crack-your-pc-and-get-paid-six-figure-fees>

تنفق روسيا وكوريا الشمالية أموالاً طائلة للحصول على أدوات «اليوم صفر». صحيفة نيويورك تايمس. نيكول بيلروث وديفيد سانغر (13 يوليو 2013). مقال: «الـ«هاكرز» يبيعون نقاط الضعف في شيفرة الكمبيوتر والدول تشتريها».

<http://www.nytimes.com/2013/07/14/world/europe/nations-buyingas-hackers-sell-computer-flaws.html>.

مكتب وزارة الدفاع (4 فبراير 2014). تقرير: «التطورات الأمنية والعسكرية في كوريا الشمالية 2013».

http://www.defense.gov/pubs/North_Korea_Military_Power_Report_2013-2014.pdf

49. دانيش دانشفيد (2 نوفمبر 2008). مقال: «السوق السوداء لثغرات «اليوم صفر» تنمو باطراد».

<http://www.zdnet.com/blog/security/black-market-for-zero-day-vulnerabilities-still-thriving/2108>

50. هناك بحوث قيّمة في ذلك الصدد. إريك ريسكورولا (7 فبراير 2005). تقرير: «هل البحث عن ثغرات أمنية فكرة جيّدة؟».

<http://www.rtfm.com/bugrate.pdf>.

ساندي كلارك (ديسمبر 2010). جامعة أوستن، ولاية تكساس. بحث: «الألفة تولّد الاحتقار: تأثير «شهر العسل» ودور إرث التشفير في ثغرات «اليوم صفر»».

26th Annual Computer Security Applications Conference, Austin, Texas,
http://dl.acm.org/citation.cfm?id=1920299

أندي أوزمنت وستيوارت شيشتر (11 مايو 2006). «مختبر لينكولن في معهد ماساشوستس للتقنية». بحث: «حليب أو نبيذ: هل يتحسن أمن البرامج الرقمية مع الزمن؟».

MIT Lincoln Laboratory,

http://research.microsoft.com/pubs/79177/milkorwine.pdf

51. ويغدو الأمر أشد سوءاً مع «إنترنت الأشياء» والبرامج المتكاملة. بروس شنابر (6 يونيو 2014). مجلة وايرد. مقال: «إنترنت الأشياء فاقدة للأمن بشكل واسع، وثغراتها غير قابلة للإغلاق».

Wired,

http://www.wired.com/2014/01/theres-no-good-way-to-patch-the-internet-of-things-and-thats-a-huge-problem

52. جيمس بول وجوليان بورغر وغلين غرينوالد (5 سبتمبر 2013). صحيفة الغارديان. مقال: «كشف أخيراً: تأثر وكالات التجسس الأمريكية والبريطانية في هزيمة الخصوصية والأمن على الإنترنت».

Guardian,

http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security

53. ظهرت النقاط الأربع في الوثيقة التالية. دانيال كاهيل (29 يوليو 2014). «خسائر الرقابة: تأثير «وكالة الأمن القومي» في الاقتصاد، حرية الإنترنت والفضاء السبراني».

http://www.newamerica.net/publications/policy/surveillance_costs_the_nsa_impact_on_the_economy_internet_freedom_cybersecurity

54. ميتشل دانيال (28 أبريل 2014). المدونة الإلكترونية للبيت الأبيض. مقال: «ثغرة «هارت بليد»: شرح عن سياق الكشف عن ثغرات سبرانية».

White House Blog,

http://www.whitehouse.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities.

55. رايان ناربان (14 سبتمبر 2010). مجلة زد نت. مقال: «هجوم «ستاكس نت» استنفذ احتياطات لدى «مايكروسوفت» تكفي 4 أيام من ثغرات «اليوم - صفر»».

ZDNet,

http://www.zdnet.com/blog/security/stuxnet-attackers-used-4-windows-zero-day-exploits/7347

56. أندريا بيترسون (4 أكتوبر 2013). صحيفة واشنطن بوست. مقال: «لماذا نصبح كلنا أقل أماناً عندما تمتنع «وكالة الأمن القومي» عن إصلاح ثغرات الأمن السبراني؟»

Washington Post,

http://www.washingtonpost.com/blogs/the-switch/wp/2013/10/04/why-everyone-is-left-lesssecure-when-the-nsa-doesnt-help-fix-security-flaws.

57. ديفيد سانغر (12 أبريل 2014). صحيفة نيويورك تايمس. مقال: «وفق رسميين: أوباما يسمح لـ «وكالة الأمن القومي» باستغلال بعض ثغرات الإنترنت».

http://www.nytimes.com/2014/04/13/us/politics/obama-lets-nsa-exploit-some-internet-flaws-officials-say.html.

كيم زيت (15 أبريل 2014). مجلة وايرد. مقال: «أوباما يقول إن «وكالة الأمن القومي» ملزمة بالكشف عن ثغرات كـ «هارت بليد»، إلا إذا كانت تستفيد منها».

Kim Zetter (15 Apr 2014),

«Obama: NSA must reveal bugs like Heartbleed, unless they help the NSA.»

Wired,

<http://www.wired.com/2014/04/obama-zero-day>.

58. جرت محاولات من ذلك القبيل. آندي أوزماند (يونيو 2005). جامعة كامبردج. بحث: «إمكانية إعادة اكتشاف ثغرة، والجدوى الاجتماعية من تصيد الثغرات».

<http://infosec.net/workshop/pdf/10.pdf>.

59. روبرت أكسلرود ورومان إليف (28 يناير 2014). مقال: «توقيت الصراع السبراني».

<http://www.pnas.org/content/early/2014/01/08/1322638111.full.pdf>.

60. هناك مقال جميل يشرح بأسلوب غير تقني «الأبواب الخلفية». سردار يوغوالاب (13 يونيو 2014). مجلة تيك ورلد. مقال: «الأبواب الخلفية الأشد ضخامة وجرأة وسوءاً في التاريخ».

Tech World,

http://www.techworld.com.au/slideshow/547475/pictures_biggest_baddest boldest_software_backdoors_all_time

61. جيمس بول وجوليان بورغر وغلين غرينوالد (5 سبتمبر 2013). صحيفة الغارديان. مقال: «كشف أخيراً: تأزر وكالات التجسس الأمريكية والبريطانية في هزيمة الخصوصية والأمن على الإنترنت».

Guardian,

<http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security>

صحيفة الغارديان، مقال (5 سبتمبر 2013). «مشروع «بول ران» دليل تصنيفي إلى برنامج وكالة الأمن القومي في كسر التشفير».

62. «وكالة الأمن القومي» (2012). «مشروع تمكين سيغينت».

<http://www.propublica.org/documents/item/784285-sigint-enabling-project.html>.

63. لورنزو فرانكيسسي-بيشياراي (11 سبتمبر 2013). موقع «ماشابل». مقال: «هل ضغطت وكالة الأمن القومي، على «مايكروسوفت» للحصول على منفذ لشيفرة برمجياتها؟»

Mashable,

<http://mashable.com/2013/09/11/fbi-microsoft-bitlocker-backdoor>.

64. جيس إمسباك (16 أغسطس 2012). شبكة «آن بي سي نيوز». «الأبواب الخلفية التي تدسها الدوافع بي أي» للرقابة، ربما تفتح أبواباً أمام الهاكرز».

NBC News,

http://www.nbcnews.com/id/48695618/ns/technology_and_science-security/t/fbi-surveillance-backdoor-might-open-door-hackers

بروس شناير (29 مايو 2013). مجلة فورين بوليسي. مقال: «الخطوة الجديدة للتنصت التي رسمتها الدوافع بي أي»، تحمل أخباراً طيبة للمجرمين».

Bruce Schneier (29 May 2013),

«The FBI's new wiretap plan is great news for criminals», *Foreign Policy*,

<http://www.foreignpolicy.com/articles/2013/05/29>

65. سوزان لاندوا (2011). كتاب: رقابة أم أمن؟ المخاطر المتأصلة من التقنيات الجديدة في التنصت.

<http://mitpress.mit.edu/books/surveillance-or-security>.

صحيفة نيويورك تايمس (21 سبتمبر 2013). مقال: «أغلقوا الأبواب الخلفية» لوكالة الأمن القومي».

New York Times,

<http://www.nytimes.com/2013/09/22/opinion/sunday/close-the-nas-back-doors.html>

66. فاسيليس بريفيلاكس ديوميدس سبينيليس (29 يونيو 2007). مقال: «القضية الأثينية».

<http://spectrum.ieee.org/telecom/security/the-athens-affair>.

67. ألكسندر سمولتسزيك (5 أكتوبر 2006). صحيفة دير شبيغل. مقال: «التجسس على «لايلا فيتا» كناية عن إيطاليا»: الإصغاء بهدوء في إيطاليا».

Der Spiegel,

<http://www.spiegel.de/international/spiegel/eavesdropping-on-la-bella-vita-listening-quietly-in-italy-a-440880.html>.

جون لايدن (14 أبريل 2008). مقال: «برياتوني يكسر الصمت بخصوص أداة التجسس على شركة «تيليكوم إيطاليا»».

http://www.theregister.co.uk/2008/04/14/telecom_italia_spying_probe_update

68. بروس شناير (23 يناير 2010). شبكة «سي أن أن». مقال: «الولايات المتحدة تمنح صينيين من اختراق «غوغل»».

CNN,

<http://www.cnn.com/2010/OPINION/01/23/schneier.google.hacking/index.html>

69. سوزان لاتناو (23 مارس 2012). مقال: «الآلة الأبدية الضخمة والقنبلة الموقوتة».

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2028152

70. البروفيسور لورانس ليسينغ (20 أكتوبر 2014). مقابلة بواسطة «يوتيوب». «الفساد المؤسساتي ووكالة الأمن القومي»: لورانس ليسينغ يحاور إدوارد سنودن».

YouTube,

<http://www.youtube.com/watch?v=DksIFG3Skb4>

71. ريان ديفيرو، غلين غرينوالد ولورا بيوتراس (19 مايو 2014). قرصنة البيانات في الكاريبي: «وكالة الأمن القومي» تسجل المكالمات الخلوية كافة في الدباهاماس».

Intercept,

<https://firstlook.org/theintercept/article/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas>

72. وكالة الأمن القومي (2012). «مشروع تمكين سيفينت».

<http://www.propublica.org/documents/item/784285-sigint-enabling-project.html>.

73. كريغ تيميرغ وأشكان سلطاني (14 ديسمبر 2013). صحيفة واشنطن بوست. «حطمت وكالة الأمن القومي» نظام التشفير للاتصالات التليفونية العامة».

Washington Post,

http://www.washingtonpost.com/business/technology/by-cracking-cellphone-code-nsa-has-capacity-for-decoding-private-conversations/2013/12/13/e119b598-612f-11e3-bf45-61f69f54fc5f_story.html.

74. دان شومو ونيلز فيرغسون (21 أغسطس 2007). شركة «مايكروسوفت». مقال: «عن إحدى الاحتمالات بشأن وجود «باب خلفي» في نظام «ويندوز»».

<http://rump2007.cr.yp.to/15-shumow.pdf>.

دي. دبليو. (18 سبتمبر 2013). موقع «كريبتوغرافي ستاك إكسستينج». مقال: «شرح للجمهور عن ضعف شيفرة «ديوالاي سي-بي آر إن»».

Cryptography Stack Exchange,

<https://crypto.stackexchange.com/questions/10417/explaining-weakness-of-dual-ec-drbg-to-wider-audience>

75. رايان غلامار وغلين غرينوالد (12 مارس 2014). موقع «إنترسبت». «خطأ وكالة الأمن القومي» لنشر برمجيات خبيثة في ملايين الحواسيب».

Intercept,

<https://firstlook.org/theintercept/article/2014/03/12/nsa-plans-infect-millions-computers-malware>.

76. غلين غرينوالد (14 يوليو 2014). موقع «إنترسبت». مقال: «سرقة استطلاعات الرأي الشبكية والطرق الأخرى التي يستخدمها جواسيس بريطانيون للسيطرة على الإنترنت».

Intercept,

<https://firstlook.org/theintercept/2014/07/14/manipulating-online-polls-ways-british-spies-seek-control-internet>.

77. بروس شناير (21 مايو 2014). موقع «شناير أون سكيوريتي». مقال: «وكالة الأمن القومي ليست سحراً». *Schneier on Security*, https://www.schneier.com/blog/archives/2014/05/the_nsa_is_not_.html
78. نيكولاس ويفر (13 مايو 2014). مجلة وايرد. مقال: «نظرة عن قرب لإحدى أقوى أدوات «وكالة الأمن القومي» لشن هجمات بواسطة الإنترنت».
- Wired*,
<http://www.wired.com/2014/03/quantum>.
Matt Brian (20 Jun 2014), «Hackers use Snowden leaks to reverse-engineer NSA surveillance devices», *Engadget*,
<http://www.engadget.com/2014/06/20/nsa-bugs-reverse-engineered>.
79. بروس شناير (4 أكتوبر 2013). صحيفة الغارديان. مقال: «الجهوم على برنامج «تور»» كيف استهدفت «وكالة الأمن القومي» إخفاء الهوية لمستخدمي الإنترنت».
- Guardian*,
<http://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity>
80. تعرّفت إلى برنامج «كوانتوم» منذ بداية تلك القصة. نيكولاس ويفر (13 مايو 2014). مجلة وايرد. مقال: «نظرة عن قرب لإحدى أقوى أدوات «وكالة الأمن القومي» لشن هجمات بواسطة الإنترنت».
- Wired*,
<http://www.wired.com/2014/03/quantum>
صحيفة دير شبيغيل (30 ديسمبر 2013). مقال افتتاحي: «وفق وثيقة لوكالة الأمن القومي»: هكذا اخترقت حسابات سرية على الإنترنت».
- Der Spiegel*,
<http://www.spiegel.de/fotostrecke/nsa-dokumente-so-uebernimmt-der-geheimdienst-fremde-rechner-fotostrecke-105329.html>.
صحيفة دير شبيغيل (30 ديسمبر 2013). مقال افتتاحي: «وفق وثيقة لوكالة الأمن القومي»: حتى جهاز الاستخبارات السري كان عرضة لاختراق إلكتروني خارجي».
- Der Spiegel*,
<http://www.spiegel.de/fotostrecke/nsa-dokumente-so-uebernimmt-der-geheimdienst-fremde-rechner-fotostrecke-105329.html>.
81. نيكولاس ويفر وروبن سومر وفينر باكسون (فبراير 2009). «منتدى عن الحوسبة الموزعة وأمن الشبكات»، جامعة «سان دييغو» بكاليفورنيا. «نقضي حزم الباكيت المزيقة لـ«بروتوكول التحكم بالبيث» على الإنترنت». Network and Distributed System Security Symposium (NDSS 2009), San Diego, California, <http://www.icir.org/vern/papers/reset-injection.ndss09.pdf>
82. مورغان ماركيز- بوار (15 أغسطس 2014). جامعة تورنتو، «مختبر المواطن»، «مركز مونك للدراسات الدولية». بحث: «شريط فيديو «قطعة شروينغر» وموت النص الصريح على الإنترنت». Citizen Lab, Munk School of Global Affairs, University of Toronto,
<https://citizenlab.org/2014/08/cat-video-and-the-death-of-clear-text>.
مورغان ماركيز- بوار (15 أغسطس 2014). موقع «إنترسيت». مقال: «سيخترق حاسوبك بمجرد مشاهدتك هذا الفيديو عن «قطعة شروينغر»».
- Intercept*,
<https://firstlook.org/theintercept/2014/08/15/cat-video-hack>.
كورا كوري ومورغان ماركيز- بوار (30 أكتوبر 2014). موقع «إنترسيت». تقرير: «كتب سرية تظهر بيع برامج تجسس رقمي للشرطة والمتسلطين في العالم».
- Intercept*,
<https://firstlook.org/theintercept/2014/10/30/hacking-team>
83. موقع «إربوين». (27 مايو 2009). برنامج «إربوين 4.0».

Sourceforge,

<http://airpwn.sourceforge.net/Airpwn.html>.

84. توم سيمونايت (19 سبتمبر 2012). مجلة معهد ماساشوسيتس للتقنية. مقال: «تقنيات «ستاكس نت» استنسخها مجرمو الكمبيوتر».

MIT Technology Review,

<http://www.technologyreview.com/news/429173/stuxnet-tricks-copied-by-computer-criminals>

85. آندي غرينبرغ (2 سبتمبر 2014). مجلة وايرد. مقال: «أداة تقنية مخصصة للبوليس، صارت أداة بيد منحرفين للحصول على صور عارية من سحابة «آي كلاود» لشركة «آبل»».

Wired,

<http://www.wired.com/2014/09/eppb-icloud>.

86. موقع شركة «موبي ستيلث» (2014). مقال: «البرنامج الرقمي الأفضل لتتبع الهواتف الخلوية».

<http://www.mobistealth.com>.

87. جاراد شير (26 فبراير 2013). شركة «سيمانتك». مقال: «دبليو32. ستاكس نت».

http://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99

88. ماثيو ي. شفارتز (12 نوفمبر 2012). مجلة إنفورميشن ويك. مقال: «نيران صديقة من «ستاكس نت»: إصابة شركة «شفرون»».

Information Week,

<http://www.darkreading.com/attacks-and-breaches/cyber-weapon-friendly-fire-chevron-stuxnetfallout/d/d-id/1107339>.

89. روبرت ماكملان (14 سبتمبر 2010). مجلة عالم الكمبيوتر. مقال: «شركة «سيمنز»: فيروس «ستاكس نت» أصاب نظاماً صناعياً».

Computer World,

http://www.computerworld.com/s/article/9185419/Siemens_Stuxnet_worm_hit_industrial_systems

90. جيفري كار (29 سبتمبر 2010). مجلة فوربس. مقال: «هل أصاب فيروس «ستاكس نت» القمر الاصطناعي الهندي «إنسات-4 بي»؟».

Forbes,

<http://www.forbes.com/sites/firewall/2010/09/29/did-the-stuxnet-worm-kill-indias-insat-4b-satellite>

91. جيمس بامفورد (13 أغسطس 2014). مجلة وايرد. مقال: «إدوارد سنودن: القصة غير المعلنة».

Wired,

<http://www.wired.com/2014/08/edward-snowden>.

92. مقال غير موقع (يوليو 2012). «أضرار جانبية لتقنية «حقن نظام أسماء النطاق» تشمل حجب الإنترنت».

<http://www.sigcomm.org/sites/default/files/ccr/papers/2012/July/2317307-2317311.pdf>

93. أيان بريمر (18 نوفمبر 2013). مجلة فورين أفيرز. مقال: «الشرعية المفقودة: لماذا صار الحوكمة أشد صعوبة مما مضى».

Foreign Affairs,

<http://www.foreignaffairs.com/articles/140274/ian-bremmer/lost-legitimacy>

94. فيفيان والت (30 يونيو 2013). مجلة تايم. مقال: «غضب عارم يجتاح رسميين أوروبيين إثر مزاعم عن تجسس «وكالة الأمن القومي» على دبلوماسيين أصدقاء لأميركا».

Time,

<http://world.time.com/2013/06/30/european-officials-infuriated-by-alleged-nsa-spying-on-friendly-diplomats>.

أن غيران (21 أكتوبر 2013). صحيفة واشنطن بوست. مقال: «تقرير عن تسجيل «وكالة الأمن القومي» الأمريكية مكالمات تليفونية لفرنسيين، يسبب صداماً دبلوماسياً أميركياً».

Washington Post,

http://www.washingtonpost.com/world/national-security/report-that-nsa-collected-french-phone-records-causing-diplomatic-headache-for-us/2013/10/21/bfa74f22-3a76-11e3-a94f-b58017bfee6c_story.html

ماثيو كارنيتشنيغ (9 فبراير 2014). صحيفة وول ستريت جورنال. مقال: «فضيحة «وكالة الأمن القومي» ترهق العلاقات مع أوروبا».

Wall Street Journal,

<http://online.wsj.com/news/articles/SB10001424052702303874504579372832399168684>

95. ديفيد إي. سانغر (1 مايو 2014). صحيفة نيويورك تايمس. مقال: «الولايات المتحدة وألمانيا تفشلان في الاتفاق بشأن التجسس».

New York Times,

<http://www.nytimes.com/2014/05/02/world/europe/us-and-germany-fail-to-reach-a-deal-on-spying>

مارك لاندر (2 أيار 2014). صحيفة نيويورك تايمس. مقال: «ميركل تشير إلى استمرار التوتر مع أميركا بشأن التجسس».

New York Times,

<http://www.nytimes.com/2014/05/03/world/europe/merkelsays-gaps-with-us-over-surveillance-remain.html>

96. خوان فوريرو (17 سبتمبر 2013). صحيفة واشنطن بوست. مقال: «فضيحة تجسس «وكالة الأمن القومي» تقصد عشاء الرئيسة البرازيلية في البيت الأبيض».

Washington Post,

http://www.washingtonpost.com/world/nsa-spying-scandal-spoils-dinner-at-the-white-house-for-brazils-president/2013/09/17/24f5acf6-1fc5-11e3-9ad0-96244100e647_story.html

الفصل 12: المبادئ

1. تتناول الكتب التالية تلك المواضيع بالنقاش. دانيال ج. سولوف (نوفمبر / ديسمبر 2007). مقال: «ليس لدي ما أخفيه، والمفاهيم المغلوطة الأخرى عن الخصوصية».

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=998565

سوزان لاندوا (2011). كتاب: رقابة أم أمن؟ المخاطر المتأتمية من التقنيات الجديدة في التنصت. <http://mitpress.mit.edu/books/surveillance-or-security>.

2. تفسر سيكولوجية الأمن كثيراً من سلوكياتنا. بروس شناير (يونيو 2008)، نص: «سيكولوجية الأمن» مداخله في منتدى سيرج فودينا «التقدم في علم التشفير: أفريكريب 2008»: المؤتمر الأول للتشفير في أفريقيا (الدار البيضاء- المغرب).

<https://www.schneier.com/paper-psychology-of-security.pdf>

دانيال غارندر (2008)، كتاب: علم الخوف: لماذا نخاف مما لا يجب خشيته، ونعرض أنفسنا لمخاطر أكبر.

The Science of Fear: Why We Fear Things We Shouldn't—And Put Ourselves in Greater Danger, Penguin, <http://books.google.com/books?id=bmyboRubog4C>.

3. بديهى القول إنَّ التكاليف تصيب الناس بصورة متفاوتة. إذ يخشى الساسة من لومهم عند حصول مجتمات

مستقبلًا، فيكون لديهم حافز لإشهار إجراءات الأمن الظاهرة. ويضحي المواطنون، خصوصاً أعضاء المجموعات السياسية والدينية المتفندة للشعبية أهدافاً واضحة للرقابة؛ لكنهم يفتقدون ما يكفي من التماسك والقوة لمقاومتها. وتتسم البرامج الواسعة في الأمن بارتفاع كلفتها، ما يعود بالفائدة على المتعاقدين مع الحكومة والساسة المؤيدين لهم.

4. في الورقة التالية، هناك محاولة لصنع نموذج عن ذلك استناداً إلى «نظرية اللعب». تيريو دراغو (فبراير 2011)، مجلة أميركان بوليتيكال ساينس ريفيو. ورقة بحث: «هل هناك مبادلة بين الأمن والخصوصية؟ الافتراضات القبلية عند السلطة التنفيذية، حماية الخصوصية ودور الإرهاب».

<http://journals.cambridge.org/download.php?file=%2FSPSR%2FS0003055410000614a.pdf&code=193cd836312527364579326df0a7aa58>

5. سوزان لاندوا (2011). كتاب: رقابة أم أمن؟ المخاطر المتأينة من التقنيات الجديدة في التنصت. <http://mitpress.mit.edu/books/surveillance-or-security>.

6. «مؤسسة الحدود الإلكترونية» (28 نوفمبر 2012). تقرير: «كيف تحمي عدم انكشاف هويتك على الإنترنت باستخدام برنامج «تور»».

https://www.eff.org/sites/default/files/filenode/Basic_Tor_Intro_Guide_FNL.pdf.

7. بالطبع، يحاول كثيرون الأمر عنه. روجر دينغلدين (30 يوليو 2014)، المدونة الإلكترونية لمشروع «تور». مقال: «مستشارية «تور»: التوصيل مبكراً، تأكيد لهجمة على الحراك الإلكتروني».

<https://blog.torproject.org/blog/tor-security-advisory-relay-early-traffic-confirmation-attack>

8. وكالة الأمن القومي (8 يناير 2007)، مذكرة «برنامج «تور» مثير للقلق». <http://cryptome.org/2013/10/nsa-tor-stinks.pdf>.

9. كيفن بولسن (5 أغسطس 2014)، مجلة وايرد. مقال: «زيارة موقع خطأ يكلفك وصول الدلاف بي أي» إلى كومبيوترك».

Wired,
http://www.wired.com/2014/08/operation_torpedo.

10. ليو كيليون (22 أغسطس 2014)، هيئة الإذاعة البريطانية. «عملاء وكالة الأمن القومي» و«القيادة الحكومية للاتصالات، سُرِّبوا الأخطاء المكتشفة في برنامج «تور»، وفق مزاعم مطوّريه».

BBC News,
<http://www.bbc.com/news/technology-28886462>.

11. أنطوني زرشير (31 أكتوبر 2013)، هيئة الإذاعة البريطانية. مقال: «من الإمبراطورية الرومانية إلى وكالة الأمن القومي»: تاريخ التجسس في العالم».

BBC News,
<http://www.bbc.com/news/magazine-24749166>

12. جون كاردويل (شتاء 1978)، مجلة دراسات الاستخبارات. مقال: «قصة من التوراة عن التجسس».

Studies in Intelligence,
<http://southerncrossreview.org/44/cia-bible.htm>

13. ثمة نقاش مهم وشائك يجب إثارته عن المخاطر النسبية للإرهاب، وقدرة الإرهاب على إحداث أضرار باستخدام التقنيات التي باتت متاحة لهم؛ لكنه أمر يتجاوز حدود الكتاب. بروس شنابير (14 مارس 2013)، مجلة وايرد. مقال: «نماذجنا عن الأمن لن تنجح أبداً، مهما فعلنا».

Wired,
<http://www.wired.com/2013/03/security-when-the-badguys-have-technology-too-how-do-we-survive>

14. بالطبع، مسألة الثقة أقل عقلانية من ذلك. بروس شنابير (2012)، كتاب: كَذِبَة ومتمردون: تفعيل الثقة التي يحتاجها المجتمع لينمو. دار «ويلي» للنشر.

<http://www.wiley.com/WileyCDA/WileyTitle/productCd-1118143302.html>.

15. في المؤسسات، هناك دوماً حاجة إلى فقايع معزولة من السرية، كي يتمكن الناس من أداء أعمالهم في المؤسسة بطريقة مناسبة، كالتصويت على مدة ولاية لجنة ما أو المداولات بصدد قرار إشكالي. إذ يؤدي جعل تلك الأشياء

- إلى إنقاص استقلالية عملية اتخاذ القرار. إذ ربما أضحي متخذو القرار أكثر اهتماماً بالشكل الذي ستبدو عليه عملية اتخاذ القرار، من اتخاذهم قراراً صائماً.
16. أدريان لي وشيلدون جاكوبسن (مايو 2012). مقال: «التنبه إلى شكوك الركاب عن المخاطر بالنسبة لمسوح الأمن في المطارات».
- <http://pubsonline.informs.org/doi/abs/10.1287/trsc.1110.0384>.
- أليسا فيكهام (7 مارس 2014). مقال: «وكالة أمن النقل» ترجى برنامجاً للتدقيق في المعلومات الشبكية عن المسافرين». مجلة لو 360.
- <http://www.law360.com/articles/516452/tsa-halts-program-to-screen-passengers-online-data>
17. أمبر توري (أبريل 2008). «جامعة براينت». مقال: «التحليل التمايزي الذي تجرته «مصلحة المداخل الداخلية» لتوقع العائد المجزي لعملية تدقيق الدخل الفردي».
- http://digitalcommons.bryant.edu/cgi/viewcontent.cgi?article=1000&context=honors_mathematics
18. تبرز تلك الإشكالية في المجتمع الشفاف الذي تخيله المفكر ديفيد برين، بمعنى أن الشفافية ليست مجانية. إذا طلب ضابط شرطة منك إبراز هويتك، لا يتحقق التوازن بأن تكون قادراً على طلب رؤية هويته. ديفيد برين (1998). دار: «بازيك بوكس». كتاب: المجتمع الشفاف: هل نرغمنا التكنولوجيا على الاختيار بين الخصوصية والحرية؟
- <http://www.davidbrin.com/transparentociety1.html>
19. صاغ «حزب قراصنة الكمبيوتر» في «أيسلندا» (نعم، إنه حزب حقيقي)، الأمر ببراءة في 2014، وقال: «حق الأفراد في الخصوصية يعني حماية الأضعف من تسلط الأقوى، كما تعني الشفافية انفتاح القوى على رقابة من لا قوة بيده». بول فونتين (19 أغسطس 2014). مجلة غرايبيفاين. مقال: «رئيس الوزراء يتعلم معنى «الشفافية»».
- <http://grapevine.is/news/2014/08/19/prime-minister-learns-what-transparency-means>
20. بالطبع، ثمة استثناءات لهذا القانون. هناك فائدة من وضع سوار تتبع إلكتروني على كواحل من أدينوا بجرائم، حتى لو أدى الأمر إلى تقليل قوة مراقبة المجرمين.
21. بيتر واتس (9 مايو 2014). بحث: «مجتمع الأرض المحروقة: دليل المفجر الانتحاري إلى الخصوصية على الإنترنت».
- <http://www.rifters.com/real/shorts/TheScorchedEarthSociety-transcript.pdf>.
22. راي سانشيز (19 يوليو 2010). شبكة «إيه بي سي نيوز». مقال: «زيادة عدد الملاحقات بسبب أجهزة فيديو للشرطة».
- <http://abcnews.go.com/US/TheLaw/videotaping-cops-arrest/story?id=11179076>.
23. تلك القرارات القانونية ليست دستورية. كاثرين مارشوسكي (25 مايو 2014). مقال: «محكمة قضت بحق رئيس «مشروع الدولة الحرة» في تسجيل بوليس دائرة «ويبر» أثناء توقف حركة المرور».
- <http://www.unionleader.com/apps/pbcs.dll/article?AID=/20140525/NEWS07/140529379>
24. ديفيد ليبسكا (27 ديسمبر 2011). موقع «سي تي إن». مقال: «عندما تسمي الشرطة استخدام كاميرات المراقبة».

CityLab,

<http://www.citylab.com/politics/2011/12/surveillance-cameras-threat-police-privacy/806>

25. سارة ليبي (18 أغسطس 2014). موقع «سيتي لاب». مقال: «إذا رأيت رجال الشرطة مرتدين كاميرات، فلا تظن أنك ستشاهداهما».

CityLab,

<http://www.citylab.com/crime/2014/08/even-when-police-do-wear-cameras-you-cant-count-on-ever-seeing-the-footage/378690>

26. كريس ماتيشيزنيك (14 أغسطس 2014). موقع «سي نت». مقال: «في «فيرغسون» ولاية «ميسوري»، الاضطراب يختبر الحق القانوني في تصوير الشرطة».

<http://www.cnet.com/news/ferguson-unrest-tests-legal-right-to-film-police>

هيل إيتالي (19 أغسطس 2014). وكالة أسوشيتدبرس. مقال: «اعتقالات «فيرغسون» تطل 10 صحفيين على الأقل».

Associated Press,

<http://abcnews.go.com/Entertainment/wireStory/ferguson-arrests-include-10-journalists-25044845>

27. بيتر سواير (يونيو 2016). جامعة بيركلي. بحث: «التناقض المستمر في دورة حياة الأسرار ومستقبل استخبارات الإشارات».

<http://www.law.berkeley.edu/plsc.htm>

28. جاكوب أبلباوم (23 أكتوبر 2013). صحيفة دير شبيغل. مقال: «برلين تشكو هل تجسست أميركا على هاتف المستشارة ميركل؟».

Der Spiegel,

<http://www.spiegel.de/international/world/merkel-calls-obama-over-suspicious-us-tappedher-mobile-phone-a-929642.html>

أيان ترينور وفيليب أولترمان وبول لويس (23 أكتوبر 2013). صحيفة الغارديان. مقال: «أنغيلا ميركل تهاتف أوباما: هل تتجسس على هاتفي الخليوي؟».

Guardian,

<http://www.theguardian.com/world/2013/oct/23/us-monitored-angelamerkel-german>.

29. هناك كتاب جيّد عن الجاسوس السوفياتي كيم فيلبي يتحدث عن جو الزوادي في وكالات التجسس. بن ماكنثاير (2014). دار «كراون». كتاب: جاسوس بين أصدقاء: كيم فيلبي والخيانة العظمى.

<http://books.google.com/books?id=wIzIAAAQBAJ>.

30. تشارلز ستروس (18 أغسطس 2013). مجلة فورين بوليسي. مقال: «سباي كيدز» [إشارة إلى فيلم هوليوودي عن اختلاف جيل الكمبيوتر عن الكبار في مهنة التجسس - المترجم].

http://www.foreignpolicy.com/articles/2013/08/28/spy_kids_nsa_surveillance_next_generation.

31. «مكتب الإدارة والميزانية» (فبراير 2014). تقرير: «مراجعة عمليات الملاءمة والأمن».

<http://www.fas.org/sgp/othergov/omb/suitsec-2014.pdf>.

32. «مدرسة أنبرغ للاتصالات والصحافة». (22 أبريل 2013). تقرير: «هل انتهت الخصوصية؟ دلائل من «مدرسة أنبرغ للاتصالات والصحافة» تشير إلى أن أجيال الألفية الثالثة يتبنون وقائع مختلفة على الإنترنت».

USC Annenberg News,

http://annenberg.usc.edu/News%20and%20Events/News/130422CDF_Millennials.aspx.

ماري مايند (21 مايو 2013). «مركز مشروع «بيو» لبحوث الإنترنت». تقرير: «مراهقون»، «سوشال ميديا» وخصوصية».

Pew Research Internet Project,

http://www.pewinternet.org/files/2013/05/PIP_TeensSocialMediaandPrivacy_PDF.pdf.

33. إنصافاً، لا نعرف إن كان ذلك يعبر عن اختلاف أساسي بين الأجيال، أو أنه مجرد معطى إحصائي تأتت «شريحة أعمار» لجيل ما زال شاباً، مع إمكان أن تتغير الصورة مع تقدّمه في العمر وتكاثر الأسرار المهمة.

34. أفكر بالسرية المؤسسية كأنها علاج كيميائي للسرطان. يصح القول إن تلك الأدوية تقتل الإنسان ببطء، لكنها تقتل السرطان بسرعة كبيرة، فيكون الفارق نافعاً بالنتيجة. إذا توصلنا إلى علاج يقتل السرطان ولا يؤثر في الإنسان، حينها نتخلّى بسرعة البرق عن العلاج الكيميائي. عندما يظهر بديل للسرية المؤسسية، يجب التخلّي عنها فوراً.
35. تشارلي روز (29 يوليو 2013). مقابلة: «الجنرال مايكل هايدن، المدير السابق لـسي آي إيه» و«وكالة الأمن القومي»، ومدير «شترف غروب».

The Charlie Rose Show,
<http://www.charlierose.com/watch/60247615>

36. نسيم نيكولاس طالب وكونستانتين سانديس (1 أكتوبر 2013). مجلة ريفيو أوف بيهيفيورال إيكونوميكس. مقال: «التجريبية في اللعبة تحمي من ذبول الحوادث».

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2298292.

37. كل مجتمع غير مبسط ومتشدد، يتعرض لسقطات كارثية. تشارلز بيرو (1984). كتاب: الحوادث الطبيعية: التعايش مع التكنولوجيات العالية المخاطر. «مطبعة جامعة برنستون».

<https://encrypted.google.com/books?id=VC5hYoMw4N0C>.

38. من الناحية النظرية، يفترض أن يحمل هذا الضرب من التفكير شفاءً. كيفن غريفين (23 سبتمبر 2011)، صحيفة هافنغتون بوست. مقال: «الخطوة 9 من الشفاء البوذي للإدمان: حرية عدم الكمال».

Huffington Post,
http://www.huffingtonpost.com/kevin-griffin/buddhist-addiction-recovery-step-9_b_958708.html

39. يعكوف ي. هايمس (أبريل 2009). المجلة الدولية لتحليل المخاطر. مقال: «عن تعريف النظم المرن».

<http://onlinelibrary.wiley.com/doi/10.1111/j.1539-6924.2009.01216.x/abstract>

40. جيس روبنز (نوفمبر 2012). مقال: «هندسة المرونة: تعلّم احتضان الفشل».

Communications of the ACM 55,
<http://queue.acm.org/detail.cfm?id=2371297>.

41. جاءت بعض الأفكار من المصدر التالي. ووريغيا يومان وجان كامب (أبريل 2013). مجلة إنوفيشن جورنال. مقال: «حماية الإنترنت من الطغاة: حلول في التقنية والسياسة لتأمين الحريات على الإنترنت».

Innovation Journal 18,
http://www.innovation.cc/scholarly-style/warigia_camp_bowman5edits18vi1a3.pdf.

42. جيمس بامفورد (2002). دار «أنكور» للنشر. كتاب: جسد الأسرار: تشريح «وكالة الأمن القومي» الفائقة السرية.

<http://www.randomhouse.com/features/bamford/author.html>.

43. جاك غولد سميث (14 أبريل 2014). موقع «لو فير». مقال: «المفارقة السريانية: كل سلاح هجومي هو (احتمالاً) جزء من نظامنا الدفاعي، والعكس بالعكس».

Lawfare,
<http://www.lawfareblog.com/2014/04/cyber-paradox-every-offensive-weapon-is-a-potential-chink-in-our-defense-and-vice-versa>

44. ستيفاني بيل وسوغويوان (15 مايو 2014). مجلة هارفرد جورنال أوف لوف أند تكنولوجي. بحث: «لم تعد «ستغفري» سراً: الاحتكار الحكومي للتلاشي للرقابة على الخلوي وتأثيره في الأمن القومي وخصوصية المستهلك».

Harvard Journal of Law and Technology (forthcoming),
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2437678

45. كيم زيتر (3 سبتمبر 2014). مجلة وايرد. مقال: «صنع «جدار نار» رقمي للهواتف يستطيع التعرّف إلى أبراج الخلوي الزائفة التي تعترض مكالماتك الهاتفية».

Wired,
<http://www.wired.com/2014/09/cryptophone-firewall-identifies-rogue-cell-towers>

أشكان سلطاني وكريغ تيمبرغ (17 سبتمبر 2014). صحيفة واشنطن بوست. مقال: «شركات التكنولوجيا ترفع الستار عن جهود الرقابة [الحكومية] في واشنطن».

Washington Post,

http://www.washingtonpost.com/world/nationalsecurity/researchers-try-to-pull-back-curtain-on-surveillance-efforts-in-washington/2014/09/17/f8c1f590-3e81-11e4-b03f-de718edeb92f_story.html

الفصل 13: حلول للحكومة

1. ريتشارد كلارك وآخرون (12 ديسمبر 2013)، «الحرية والأمن في عالم متغير: تقرير وتوصيات «لجنة الرئاسة للمراجعة بشأن الاستخبارات وتقنيات الاتصالات»، المكتب التنفيذي للرئيس الأمريكي.
http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.
2. «مؤسسة الحدود الإلكترونية» (مايو 2014) تقرير: «ضروري ومناسب: مبادئ دولية لتطبيق حقوق الإنسان على رقابة الاتصالات: عرض خلفية الموضوع والتحليل القانوني المساند».
<https://en.necessaryandproportionate.org>.
3. «مؤسسة الحدود الإلكترونية» (5 يناير 2014) تقرير: «13 مبدأ دولياً لتطبيق حقوق الإنسان على رقابة الاتصالات».
<https://necessaryandproportionate.org/files/2014/01/05/13p-onepagerfinal.pdf>.
4. في مثل واحد على ذلك، قال جيمس كلايبر، رئيس الاستخبارات القومية، إن «الكشف عن معلومات حول الطرق المحددة التي تستعملها الحكومة لجمع بيانات الاتصالات، بإمكانه بوضوح أن يعطي أعداءنا ما يشبه «كتاب قواعد اللعب» لتجنب اكتشافهم [من قبل الحكومة]». صحيفة نيويورك دايلي نيوز نقلاً عن وكالة أسوشيتدبرس في (9 يونيو 2013)، مقال: «دفاع رئيس الاستخبارات جيمس كلايبر عن برنامج التجسس على الإنترنت».
- New York Daily News,
<http://www.nydailynews.com/news/politics/intelligence-chief-james-clapper-defends-internet-spying-program-article-1.1367423>.
5. في العام 2014، علمنا أن إسرائيل تنصّت على الاتصالات الدبلوماسية بين وزير الخارجية جون كيري ودول مختلفة في الشرق الأوسط. صحيفة دير شبيغيل (3 أغسطس 2014). مقال افتتاحي: «تنصّت: إسرائيل تسترق السمع إلى محادثات كيري في الشرق الأوسط».
- Der Spiegel,
<http://www.spiegel.de/international/world/israel-intelligence-eavesdropped-on-phone-calls-by-john-kerry-a-984246.html>
6. كونور فريدرسدورف (18 مارس 2014). مجلة أتلانتيك. مقال: «لماذا لا يوصف التعديل الرابع في الدستور بأنه سري؟».
- Atlantic,
<http://www.theatlantic.com/politics/archive/2014/03/why-isnt-the-fourth-amendment-classified-as-top-secret/284439>
7. لننذكر أيضاً أن معظم ذلك تأتّى كرد فعل على إساءة الشرطة استعمال السلطة. ليس الأمر أن الشرطة أقل ميلاً لإساءة استخدام السلطة، بل إننا امتلكتنا من الوقت ما كان كافياً لتطوير قوانين للسيطرة عليه.
8. بروس شناير (31 يوليو 2012)، شبكة «سي أن أن». مقال: «استنتاج دروس مغلوطة من أحداث مخيفة».
- CNN,
<http://www.cnn.com/2012/07/31/opinion/schneier-aurora-aftermath/index.html>
9. يطلق تقنيو الأمن المعلوماتي على النظم الرقمية غير الشفافة تسمية «الأمن بالتعمية». إذ يكون التصميم الجيد للنظم إلى عكس ذلك، بمعنى أنها تكون فعّالة حتى لو علم الجميع بتفاصيلها كافة. بروس شناير (15 مايو 2002). كتاب كريبتو غرام: السرية، الأمن والتعمية.
- Crypto-Gram,

<https://www.schneier.com/crypto-gram-0205.html#1>.

10. مايكل سيلفلين (سبتمبر 2009). مجلة منظمة الصحة العالمية. تقرير: «سيطرة البحوث المزدوجة الاستخدام: إشكالية أخلاقية».

Bulletin of the World Health Organization 87,

<http://www.who.int/bulletin/volumes/87/9/08-051383/en>

- كارل زيمر (5 مارس 2012). صحيفة نيويورك تايمس. مقال: «الهواة مصدر خوف جديد في صنع فيروسات متحولة».

New York Times,

<http://www.nytimes.com/2012/03/06/health/amateur-biologists-are-new-fear-in-making-mutant-flu-virus.html>.

- مايكل سبكت (12 مارس 2012). صحيفة نيويورك. مقال: «الفيروس الأشد فتكاً».

New Yorker,

<http://www.newyorker.com/magazine/2012/03/12/the-deadliest-virus>

11. بيث كاسبر (أغسطس 2001). «مركز الاستراتيجية والتكنولوجيا» في «كلية الحرب الجوية». ورقة بحث: «نهاية السرية؟ التنافس العسكري في عصر الشفافية».

Strategy and Technology, Air War College, Air University, Maxwell Air Force Base, Alabama,

<http://www.fas.org/sgp/eprint/kaspar.pdf>.

12. «وكالة الأمن القومي» (31 أكتوبر 2013). تقرير: «نشاطات ووكالة الأمن القومي»: التركيز على الأهداف المتوقعة من [أفراد] الاستخبارات الأجنبية».

http://www.nsa.gov/public_info/press_room/2013/NSA_Activities_Valid_FI_Targets.pdf

13. في أحد تلك الآراء، لاحظ القاضي بايتس «أن ووكالة الأمن القومي» تجاوزت باستمرار المدى المخول لها في المصادر. سبتمبر [إكرمان (19 نوفمبر 2013). صحيفة الغارديان. مقال: «الكشف للمرة الأولى عن القرار القضائي من محكمة «فيضاء» الذي أتاح لوكالة الأمن القومي» ممارسة الرقابة».

Guardian,

<http://www.theguardian.com/world/2013/nov/19/court-order-that-allowed-nsa-surveillance-is-revealed-for-first-time>

- يوشاي بنكر (16 أكتوبر 2013). صحيفة الغارديان. مقال: «كيف تفسد الدوافع بي أي» و«وكالة الأمن القومي» إشرافاً [حكومياً] ضعيفاً».

Yochai Benkler (16 Oct 2013), «How the NSA and FBI foil weak oversight», *Guardian*,

<http://www.theguardian.com/commentisfree/2013/oct/16/nsa-fbi-endrun-weak-oversight>

- مارسي ويلر (22 أغسطس 2014). مجلة ويك. مقال: «لهذه الأسباب، لا تستطيع الثقة بـوكالة الأمن القومي»، أبدأ».

Week,

<http://theweek.com/article/index/266785/this-is-why-you-cant-trust-the-nsa-ever>

14. بيتر ولستن (10 أغسطس 2013). صحيفة واشنطن بوست. مقال: «محامون يقولون إن عوائق انتصبت في وجه الإشراف على برنامج «وكالة الأمن القومي» في رقابة الهواتف».

Washington Post,

http://www.washingtonpost.com/politics/2013/08/10/bee87394-004d-11e3-9a3e-916de805f65d_story.html.

15. غلين غرينوالد (4 أغسطس 2013). صحيفة الغارديان. مقال: «أعضاء في الكونغرس يمنعون من معلومات أساسية عن «وكالة الأمن القومي»».

Guardian,

<http://www.theguardian.com/commentisfree/2013/aug/04/congress-nsa-denied-access>

16. إلزا تشانغ (11 يونيو 2013). موقع «أولتغز كونسدرد». مقال: «ما الذي يعرفه الكونغرس حقاً عن ترصد وكالة الأمن القومي؟».

All Things Considered, NPR,

<http://www.npr.org/blogs/itsallpolitics/2013/06/11/190742087/what-did-congress-really-know-about-nsatracking>.

17. رون وايدن (29 يناير 2014). «خطاب وايدن أثناء جلسة استماع مفتوحة في مجلس الشيوخ».

<http://www.wyden.senate.gov/news/press-releases/wyden-statement-at-senate-intelligence-committees-open-hearing>

18. ديانا فاينشتاين (28 أكتوبر 2013). تقرير: «خطاب ديانا فاينشتاين بشأن جمع الاستخبارات بيانات عن قادة أجنبية».

<http://www.feinstein.senate.gov/public/index.cfm/2013/10/feinstein-statement-on-intelligence-collection-of-foreign-leaders>.

19. آلان غرايسون (25 أكتوبر 2013). صحيفة الغارديان. مقال: «إشراف الكونغرس على وكالة الأمن القومي» هو نكتة. أنا أعرف ذلك، فأنا في الكونغرس».

Guardian,

<http://www.theguardian.com/commentisfree/2013/oct/25/nsa-no-congress-oversight>

20. بروس شنابير (16 يناير 2014). مدونة إلكترونية. مقال: «اليوم، قدّمت تلخيصاً للكونغرس عن وكالة الأمن القومي».

21. بيتر ولسطن (10 أغسطس 2013). صحيفة واشنطن بوست. مقال: «محامون يقولون إن عوائق انتصبت في وجه الإشراف على برنامج وكالة الأمن القومي» في رقابة الهواتف».

Washington Post,

http://www.washingtonpost.com/politics/2013/08/10/bee87394-004d-11e3-9a3e-916de805f65d_story.html.

22. جون نابير تاي (18 يوليو 2014). صحيفة واشنطن بوست. مقال: «شرح عن الأمر التنفيذي رقم 12333: قانون ريفان الذي أطلق يد وكالة الأمن القومي» في التجسس على الأميركيين».

http://www.washingtonpost.com/opinions/meet-executive-order-12333-the-reagan-rule-that-lets-the-nsa-spy-on-americans/2014/07/18/93d2ac22-0b93-11e4-b8e5-d0de80767fc2_story.html

تشارلي سافاج وآيشيا بارلينو (13 أغسطس 2014). صحيفة نيويورك تايمس. مقال: «مجموعتان متباينتان من القوانين للرقابة، إحداها للأميركا والثانية للأراضي الأجنبية».

New York Times,

<http://www.nytimes.com/interactive/2014/08/13/us/two-sets-of-rules-for-surveillance.html>.

ألين ناكاشيما وأشكان سلطاني (23 يوليو 2014). صحيفة واشنطن بوست. مقال: «الهدف التالي لمؤسسة تدافع عن الخصوصية: الملح الأضخم والأقل ظهوراً في رقابة وكالة الأمن القومي».

Washington Post,

<http://www.washingtonpost.com/blogs/the-switch/wp/2014/07/23/privacywatchdogs-next-target-the-least-known-but-biggest-aspect-of-nsa-surveillance>

تشارلي سافاج (13 أغسطس 2014). صحيفة نيويورك تايمس. مقال: «وفق مساعد سابق: قانون للرقابة من زمن ريفان يتعدى على الحقوق».

New York Times,

<http://www.nytimes.com/2014/08/14/us/politics/reagan-era-order-on-surveillance-violates-rights-says-departing-aide.html>.

23. أليكس أبديو (29 سبتمبر 2014)، «وثائق جديدة تلقي الضوء على أقوى أدوات «وكالة الأمن القومي»».

Free Future,

<https://www.aclu.org/blog/national-security/new-documents-shed-light-one-nsas-most-powerful-tools>

24. مارسيل ويلر (7 ديسمبر 2007)، موقع «إيميتي ويل»، مقال: «البيت الأبيض يضبط متلبساً بتهمة الادعاء بعدم وجود قانون يضبطه».

Empty Wheel,

<https://www.emptywheel.net/2007/12/07/whitehouse-rips-the-white-house>

25. جوستين إليوت (17 يونيو 2013)، موقع «بروبابليكا»، مقال: «أندكّر أيام انحصر النقاش عن «قانون باتريوت» بسجلات المكتبات؟»

Pro Publica,

<http://www.propublica.org/article/remember-when-the-patriot-act-debate-was-about-libraryrecords>

26. مايك مازنيك (17 سبتمبر 2013)، موقع «تيك درت»، مقال: «المحاكم تكشف «تفسيراً سريعاً» لـ«قانون باتريوت»، يتيح لـ«وكالة الأمن القومي» جمع بيانات الهواتف كلها».

Tech Dirt,

<https://www.techdirt.com/articles/20130917/13395324556/court-revealssecret-interpretation-patriot-act-allowing-nsa-to-collect-all-phone-call-data.shtml>

27. أندريا بيترسون (11 أكتوبر 2013)، صحيفة «واشنطن بوست»، مقال: «مؤلف «قانون باتريوت»: هناك فشل في الإشراف».

Washington Post,

<http://www.washingtonpost.com/blogs/the-switch/wp/2013/10/11/patriot-act-author-therehas-been-a-failure-of-oversight>.

28. جينيفر فالنتينو-ديفريرز وسيويهان غورمان (8 يوليو 2013)، صحيفة «ول ستريت جورنال»، مقال: «إعادة تعريف محكمة سرية لكلمة «دلالة»، أعطت «وكالة الأمن القومي» سلطات واسعة في جمع البيانات».

Wall Street Journal,

<http://online.wsj.com/news/articles/SB10001424127887323873904578571893758853344>

29. مجلس الشيوخ الأمريكي (26 أبريل 1976)، وثيقة حكومية: «التقرير النهائي للجنة المنتدبة لدراسة عمليات الحكومة المتصلة بنشاطات الاستخبارات. تأثير رقابة «وكالة الأمن القومي» في الأمريكيتين».

http://www.aarclibrary.org/publib/church/reports/book3/pdf/ChurchB3_10_NSA.pdf

30. كاسبر باودن (23 أغسطس 2012)، تقرير: «إقرار إلى «اللجنة المشتركة» بصدد مسودة «مشروع قانون بيانات الاتصالات»».

http://www.academia.edu/6002584/Submission_to_the_Joint_Committee_on_the_draft_Communications_Data_Bill

31. أثناء منازعة قانونية حديثة، وصفه قاضٍ بأنه «قانون صعب، بل لا نفاذ إلى مرماه»، وسماه مدعي عام الحكومة نفسها بأنه «تشريع ملوئ بالالتفافات». «أوين بوكوت (18 يوليو 2014)، صحيفة «الغارديان»، مقال: «الاستخبارات تصنع قواعد بيانات ضخمة من البريد الإلكتروني الذي تعترضه على الإنترنت».

Guardian,

<http://www.theguardian.com/uk-news/2014/jul/18/intelligence-services-email-database-internet-tribunal>.

32. تنطبق قوانين «الاتحاد الأوروبي» على المملكة المتحدة، وتعتمد الرقابة العامة تحت مظلة «قانون تنظيم سلطات التحقيق»، على «الميثاق الأوروبي لحقوق الإنسان». نيك هوبكنز (28 يناير 2014)، صحيفة «الغارديان»، مقال:

«المظلة الواسعة للرقابة العامة لقيادة الحكومة للاتصالات»، هي غير شرعية وفق محام رفيع المستوى».

Guardian,
<http://www.theguardian.com/uk-news/2014/jan/28/gchqmass-surveillance-spying-law-lawyer>.

33. قال الرئيس أوباما إنَّ برامج «وكالة الأمن القومي» تجري «في ظل إشراف دقيق من الأذرع الثلاث للحكم». باراك أوباما (7 يونيو 2013)، صحيفة وول ستريت جورنال، «مقتطفات من ملاحظات أوباما عن الجدل بشأن وكالة الأمن القومي».

Wall Street Journal,
<http://blogs.wsj.com/washwire/2013/06/07/transcript-whatobama-said-on-nsa-controversy>

34. «مركز معلومات الخصوصية الإلكترونية» (2014). تقرير: «قرارات المحاكم بشأن قانون مراقبة الاستخبارات الأجنبية: 1979-2014».

https://epic.org/privacy/wiretap/stats/fisa_stats.html

35. أشار «الاتحاد الأمريكي للحريات المدنية» نقاشاً واسعاً عن ضرورة الإصلاح وأسبابها. «الاتحاد الأمريكي للحريات المدنية» (2014). نداء: «أصلحو البند 215 من «قانون باتريوت»».

<https://www.aclu.org/free-speech-national-security-technology-and-liberty/reform-patriot-act-section-215>

36. ناقش «الاتحاد الأمريكي للحريات المدنية» أيضاً، الحاجة إلى إحداث إصلاح يتناول ذلك الأمر. جميل جعفر (19 مارس 2014). «إقرار من جميل جعفر، نائب المدير القانوني في «الاتحاد الأمريكي للحريات المدنية»، عن جلسة الاستماع العام لـهيئة الإشراف على الخصوصية والحريات المدنية»، حول البند 702 من «قانون تعديلات عمل محكمة فيسا».

http://www.pclob.gov/Library/Meetings-Events/2014-March-19-Public-Hearing/Testimony_Jaffer.pdf

37. جرى حوار متبادل في «لجنة الاستخبارات» في مجلس الشيوخ، بين السيناتور رون وايدن (عن ولاية «أوريغون»)، ومدير «وكالة الأمن القومي» حينها، ألكسندر كيث. ووجه وايدن إلى ألكسندر سؤالاً عن جميع الوكالة بشكل واسع لـالبيانات المكانية من هواتف الأميركيين. ورد ألكسندر بأن الوكالة لم تجمعها تحت السلطة المناطة بها بموجب البند 215 من «قانون باتريوت». عندها، سأل وايدن من ألكسندر إيضاح إذا كانت الوكالة جمعت تلك البيانات بموجب تحويل قانوني آخر. ورفض ألكسندر الإجابة. روبن غرين (27 سبتمبر 2013). صحيفة واشنطن مارك أب. مقال: «رسمياً: تريد «وكالة الأمن القومي» اغتشاف بيانات هواتف الأميركيين كافة».

Washington Markup,
<https://www.aclu.org/blog/national-security/its-official-nsa-wants-suck-all-americans-phonerecord>

38. مارسي ويلر (14 أغسطس 2014). موقع «إيميتي ويل». مقال: «معظم الأوامر المتعلقة بالبند 215، تتناول شركات إنترنت رفضت رسائل طلب كشف المعلومات من «وكالة الأمن القومي»».

Empty Wheel,
<http://www.emptywheel.net/2014/08/14/the-bulk-of-215-orders-come-from-internet-companies-that-refuse-nsa>

39. مارسي ويلر (23 يونيو 2014). مقال: «نظرية الذراع الوحيد في الإشراف». <http://www.cato-unbound.org/2014/06/23/marcy-wheeler/single-branch-theory-oversight>

40. ريتشارد كلارك وآخرون (12 ديسمبر 2013)، «الحرية والأمن في عالم متغير: تقرير وتوصيات لجنة الرئاسة للمراجعة بشأن الاستخبارات وتقنيات الاتصالات»، المكتب التنفيذي للرئيس الأمريكي.

http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

41. باراك أوباما (17 يناير 2014). المكتب التنفيذي للرئاسة. تقرير: «ملاحظات من الرئيس عن لجنة مراجعة الاستخبارات».
- US Executive Office of the President,
<http://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signalsintelligence>
42. غاريت هاتش (27 أغسطس 2012). «خدمة بحوث الكونغرس». تقرير: «هيئة الإشراف بصدد الخصوصية والحريات المدنية الوضع الجديد المستقل للوكالة».
- Congressional Research Service,
<http://www.fas.org/sgp/crs/misc/RL34385.pdf>.
43. «الاتحاد الأمريكي للحريات المدنية» (2 يوليو 2014). تقرير: «هيئة إشراف حكومي تشير إلى غياب السند القانوني لكثير مما يتصل ببرنامج المراقبة في «وكالة الأمن القومي»».
- <https://www.aclu.org/national-security/government-privacy-watchdogsigns-much-nsa-warrantless-wiretapping-program>
44. «هيئة الإشراف بصدد الخصوصية والحريات المدنية» (2 يوليو 2014). وثيقة: «تقرير عن برنامج المراقبة الممارس بموجب البند 702 من «قانون مراقبة الاستخبارات الأجنبية»».
- <http://www.pclob.gov/All%20Documents/Report%20on%20the%20Section%20702%20Program/PCLOB-Section-702-Report.pdf>
45. فريدريك أ. و. شفارتز جونيور (12 مارس 2014). صحيفة نايشن. مقال: «لماذا نحتاج إلى «شيرش كومي تي» لإصلاح نظامنا الاستخباراتي الفاشل».
- Nation*,
<http://www.thenation.com/article/178813/why-we-need-new-church-committee-fixour-broken-intelligence-system>
46. هناك مثلٌ عن ذلك في الموضوع التالي. غريغوري كونتي وليزا شاي وودرو هارتزوغ (صيف 2014). مقال: «تفكيك العلاقة بين الخصوصية والأمن».
- <http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6824305>.
47. جميل جعفر (19 مارس 2014). «إقرار من جميل جعفر، نائب المدير القانوني في «الاتحاد الأمريكي للحريات المدنية»، عن جلسة الاستماع العام لـهيئة الإشراف على الخصوصية والحريات المدنية»، حول البند 702 من «قانون تعديلات عمل محكمة فيسا».
- http://www.pclob.gov/Library/Meetings-Events/2014-March-19-Public-Hearing/Testimony_Jaffer.pdf
48. مؤسسة «برايفسي إس أو إس» (10 ديسمبر 2013). تقرير: «لا أدلة، لا قلق: عن استعمال مذكّرات الجلب السريّة».
- <http://www.privacycos.org/node/1263>
49. أندرو نولان وريتشارد م. توميسون الثاني وفيفيان س. شو (25 أكتوبر 2013). «خدمة بحوث الكونغرس». تقرير: «تعريف محامٍ عن العموم بالحاكم المختصة بـ«قانون مراقبة الاستخبارات الأجنبية»: انتقاء القضايا القانونية».
- <http://fas.org/sgp/crs/intel/advocate.pdf>.
- كونفغتون وبرلينغ (مايو 2014). موقع «إنسايد برايفسي». مقال: «عن دستورية وجود محامٍ عن العموم لشؤون الخصوصية».
- <http://www.insideprivacy.com/files/2014/07/The-Constitutionality-of-a-Public-Advocate-for-Pri.pdf>
50. جويل رايندرغ (2 نوفمبر 2013). ورقة (تحت الطبع): «حال بيانات المراقبة في أوروبا وأمريكا».
- http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2349269.
51. إدوارد سنودن (7 مارس 2014). «بيان إلى البرلمان الأوروبي».
- <http://www.europarl.europa.eu/document/activities/cont/201403/20140307ATT80674/20140307ATT80674EN.pdf>

52. ميرك بوب (16 نوفمبر 2005). تقرير: «الإشراف الداخلي والخارجي على الشرطة في الولايات المتحدة». http://www.parc.info/client_files/altus/10-19%20altus%20conf%20paper.pdf.
53. مايكل ب. فاينيك (3 يونيو 2010). مقال: «المراقبة على المراقبين: دروس للقوى الفيدرالية لإنفاذ القانون، من المدن الأميركية». <http://www.wmtchell.edu/lawreview/documents/12.weinbeck.pdf>
إدوارد ل. كالدرون وماريا هرنانديز- فيغورا (يناير 2013). جامعة كاليفورنيا. مقال: «دور جمعيات المواطنين في الإشراف على قوى إنفاذ القانون». http://cpp.fullerton.edu/cpp_policeoversight_report.pdf.
54. ديفيد بوزن (20 ديسمبر 2013). مجلة هارفرد لوفريغو. مقال: «وحش ليفيathan المُسرَّب: كيف تدين الحكومة وتشجع الكشف غير المشروع عن الوثائق». *Harvard Law Review* 127, <http://harvardlawreview.org/2013/12/the-leaky-leviathan-why-the-government-condemns-and-condones-unlawful-disclosures-of-information>.
راهول ساغار (20 ديسمبر 2013). مجلة هارفرد لوفريغو. مقال: «صير ليفيathan المُسرَّب: تعليق على فكرة ديفيد بوزن عن وحش ليفيathan المُسرَّب». *Harvard Law Review Forum* 127, http://cdn.harvardlawreview.org/wp-content/uploads/pdfs/forvol127_sagar.pdf.
55. يعرض المقالان التاليان ذلك الموضوع. دانا بويد (19 يوليو 2013). موقع «آبوفينا». مقال: «إطلاق صافرات الإنذار بوصفه شكلاً جديداً للعصيان المدني: عن أهمية سنودن». *apophenia*, <http://www.zephor.org/thoughts/archives/2013/07/19/edwardsnowden-whistleblower.html>
ويليام ي. شويارمان (سبتمبر 2014). موقع «الفلسفة والنقد الاجتماعي». مقال: «إطلاق صافرة الإنذار بوصفه تمرّداً مدنيّاً: حال إدوارد سنودن». *Philosophy and Social Criticism* 40, <http://psc.sagepub.com/content/40/7/609.abstract>.
56. ج. أليكس سنها (28 يوليو 2014). مؤسسة «هيومن رايتس ووتش». مقال: «لديهم حرية أن يراقبوا الجميع». Human Rights Watch, <http://www.hrw.org/reports/2014/07/28/libertymonitor-all>.
57. راهول ساغار (2013). «مطبوعة جامعة برنستون». كتاب: أسرار وتسرّيات: الإشكالية في سرية الدولة. <http://press.princeton.edu/titles/10151.html>
58. ماري- روز بابتدريا (مارس 2014). مجلة بوسطن يونيفرسيتي لوفريغو. مقال: «مُسرَّب خائن مُطلق صافرة إنذار جاسوس: تسريبات «وكالة الأمن القومي» والتعديل الأول للدستور الأمريكي». <http://www.bu.edu/bulawreview/files/2014/05/PAPANDREA.pdf>
59. بروس شنابير (6 يونيو 2013). مجلة «أتلانتيك». مقال: «ما لا نعرفه عن التجسس على المواطنين: إنهم أشدّ ذعراً مما نعرف». *Atlantic*, <http://www.theatlantic.com/politics/archive/2013/06/what-we-dont-know-about-spying-on-citizensscarier-than-what-we-know/276607>
60. قَدَم يوشاي بنكر مؤشرات تستطيع المحاكم الاستناد إليها في تقرير ذلك. يوشاي بنكر (يوليو 2014). مجلة هارفرد ريفيو أوف لوفريغو أوف لوفريغو. بحث: «دفاع من وجهة الموثوقية الشعبية عن تسريبات وثائق وكالة الأمن القومي» ومُطلق صافرات الإنذار بشأنها». *Harvard Review of Law and Policy* 8, http://benkler.org/Benkler_Whistleblowerdefense_Prepub.pdf

61. يتبنّى يوشاي بنكر فكرة أن الشيء الأشدّ نكأة الذي يجب على الولايات المتحدة فعله، هو إعطاء إدوارد سنودن حصانة قانونية، والسماح له بالعودة إلى الولايات المتحدة. يوشاي بنكر (8 سبتمبر 2014). مجلة أتلانتيك. مقال: «أنتريدون إصلاح «وكالة الأمن القومي»؟ إذا، أعطوا إدوارد سنودن حصانة قانونية».
62. وزارة العمل (2014). يملك غلين راينولدز أفكاراً عن تعظيم الفائدة من إطلاق صافرة الإنذار إلى الحدّ الأقصى، مع تخفيض الأدنى إلى الحدّ الأدنى. غلين راينولدز (15 سبتمبر 2014). شبكة بحوث العلوم الاجتماعية. مقال: «لا تخشى مُطلق صافرة الإنذار: أفكار عن البيروقراطية والإطلاق الأخلاقي لصافرات الإنذار».

Social Sciences Research Network,
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2496400

63. أكسل آرنيك (30 سبتمبر 2013). «مجلس الخصوصية والرقابة- لوزان، سويسرا». مقال: «السؤال الذي لا يطرحه المحامون: هل يستطيع القانون تأييد رقابة انتقالية شاملة؟».

Congress on Privacy and
 Surveillance, Lausanne, Switzerland,
<http://ic.epfl.ch/privacy-surveillance>

64. بن إمرسون (23 سبتمبر 2014). الجمعية العامة للأمم المتحدة في دورتها 69. تقرير المقرر الخاص بشأن نشر وحماية حقوق الإنسان والحريات الأساسية أثناء مكافحة الإرهاب.
<https://docs.google.com/document/d/18U1aHmKx9jFDQjCZeAUyZdRjI6iF4QjuSaJO2Uy7NY/edit?pli=1>.
65. كيم زيت (22 أكتوبر 2013). مجلة وايرد. مقال: «محكمة تقضي بضرورة الحصول على إذن مستند إلى وجود مشتبّه فيه محتمل، لتفعيل مجسّات الدجبي بي إس».

Wired,
<http://www.wired.com/2013/10/warrant-required-gps-trackers>.

66. روبرت بارنز (25 يونيو 2014). صحيفة واشنطن بوست. مقال: «المحكمة العليا تلزم الشرطة الحصول على مذكرات قضائية في معظم أحوال تفتيش الخولي».

Washington Post,
http://www.washingtonpost.com/national/supreme-court-police-must-get-warrants-for-most-cellphoneseaches/2014/06/25/e2ff1326-fc6b-11e3-8176-f2c941cf35f1_story.html.

67. أودين كير وغريغ نجيم (1 أغسطس 2012). مجلة إيه بي إيه. مقال: «مسألة البيانات: هل يجب إعادة النظر في نظام الطرف الثالث؟».

http://www.abajournal.com/magazine/article/the_data_question_should_the_third-party_records_doctrine_be_revisited.

ريتشارد م. تومبسون الثاني (5 يونيو 2014). «خدمة بحوث الكونغرس». تقرير: «التعديل الرابع في الدستور ونظام الطرف الثالث».

Congressional Research Service,
<http://fas.org/sgp/crs/misc/R43586.pdf>

68. حاضراً، فإنّ القاضي [سونيا] سوتومايور هي الوحيدة في «المحكمة العليا» التي كتبت تأييداً لإدخال تلك التعديلات. ريتشارد م. تومبسون الثاني (5 يونيو 2014). «خدمة بحوث الكونغرس». تقرير: «التعديل الرابع في الدستور ونظام الطرف الثالث».

Congressional Research Service,
<http://fas.org/sgp/crs/misc/R43586.pdf>

69. في 2014، استخدم الروس إحدى ثغرات «اليوم- صفر» في نظام «ويندوز» كي يتجسسوا على حلف الدناتو، والحكومة الأوكرانية. ألين ناكاشيما (13 أكتوبر 2014). صحيفة واشنطن بوست. مقال: «استخدم «هاكرز» روس ثغرات «اليوم- صفر» للاختراق الدناتو وأوكرانيا، ضمن حملة تجسس سبراني».

Washington Post,

http://www.washingtonpost.com/world/national-security/russian-hackers-use-zero-day-to-hack-nato-ukraine-in-cyberspy-campaign/2014/10/13/t2452976-52f9-11e4-892e-602188e70e9c_story.html

70. كوري دوكتورو (11 مارس 2014). صحيفة الغارديان. مقال: «إذا أرادت القيادة الحكومية للاتصالات، تحسين الأمن القومي، يجب عليها إصلاح تقنياتها».

Guardian,

<http://www.theguardian.com/technology/2014/mar/11/gchq-national-security-technology>.

Dan Geer (2013), «Three policies»,

<http://geer.tinho.net/three.policies.2013Apr03Wed.PDF>

71. ديفيد ي. سانغر (29 أبريل 2014). صحيفة نيويورك تايمس. مقال: «البيت الأبيض يشرح تفكيره بشأن الاختلالات في الأمن السبراني».

New York Times,

<http://www.nytimes.com/2014/04/29/us/white-house-details-thinking-on-cybersecurity-gaps.html>.

72. كانت تلك التوصية رقم 30 من تلك اللجنة. ريتشارد كلارك وآخرون (12 ديسمبر 2013)، «الحرية والأمن في عالم متغير: تقرير وتوصيات لجنة الرئاسة للمراجعة بشأن الاستخبارات وتقنيات الاتصالات»، المكتب التنفيذي للرئيس الأمريكي، ص 187.

http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

73. بروس شنابر (19 مايو 2014). صحيفة أتلانتيك. مقال: «هل يجب على الدهاكرز الأميركيين إصلاح ثغرات الأمن السبراني أم الاستفادة منها؟».

Atlantic,

<http://www.theatlantic.com/technology/archive/2014/05/should-hackers-fix-cybersecurity-holes-or-exploitthem/371197>.

74. ميتشل دانيال (28 أبريل 2014). المدونة الإلكترونية للبيت الأبيض. مقال: «ثغرة «هارت بليد»: شرح عن سياق الكشف عن ثغرات سبرانية».

White House Blog,

<http://www.whitehouse.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities>.

ديفيد ي. سانغر (29 أبريل 2014). صحيفة نيويورك تايمس. مقال: «البيت الأبيض يشرح تفكيره بشأن الاختلالات في الأمن السبراني».

New York Times,

<http://www.nytimes.com/2014/04/29/us/white-house-details-thinking-on-cybersecurity-gaps.html>.

كريستوفر جوي (8 مايو 2014). صحيفة استراليا إن فايننشال ريفيو. مقال: «نص مقابلة: الرئيس السابق لدوكالة الأمن القومي» وقائد «القيادة السبرانية الأمريكية»، الجنرال كيث ألكسندر».

Australian Financial Review,

<http://www.afr.com/Page/Uuid/b67d7b3e-d570-11e3-90e8-355a30324c5f>.

75. بروس شنابر (5 سبتمبر 2013). صحيفة الغارديان. مقال: «الحكومة الأمريكية خانت الإنترنت. نحتاج إلى استرداد ثقتها».

Guardian,

<http://www.theguardian.com/commentisfree/2013/sep/05/government-betrayed-internet-nsa-spying>

ستيفان فاريل (2013). مقال: «الرقابة الواسعة هي هجوم سبراني».

<http://tools.ietf.org/pdf/draft-farrellperpass-attack-00.pdf>.

76. شارلي سافاج (27 سبتمبر 2010). صحيفة نيويورك تايمس. مقال: «الولايات المتحدة تحاول تسهيل التنصت على الإنترنت».

New York Times,

<http://www.nytimes.com/2010/09/27/us/27wiretap.html>

رايان سنغل (17 فبراير 2011). مجلة وايرد. مقال: «الحذف بي أي» تضغط لفرض «أبواب خلفية» للرقابة في أدوات «ويب 2.0».

Wired,

<http://www.wired.com/2011/02/fbi-backdoors>

فاليري كابروني (17 فبراير 2011). «خطاب أمام اللجنة الفرعية في مجلس النواب، للجريمة والإرهاب والأمن الوطني».

<http://www.fbi.gov/news/testimony/going-dark-lawful-electronic-surveillance-in-the-face-of-new-technologies>

77. ليس أمراً جديداً. ففي ثمانينيات القرن العشرين وتسعينياته، كانت «وكالة الأمن القومي» تدس «أبواباً خلفية» في شيفرة منتجات إلكترونية تباعها شركة «كريبتو إيه. جي» السويسرية. سكوت شاين وتوم بومان (4 ديسمبر 1995). صحيفة بالتيموور صن. مقال: «تخريب اللعبة».

<http://cryptome.org/jya/nsa-sun.htm>.

78. كريستوفر كيتشام (27 سبتمبر 2008). موقع «كاونتر بنش». مقال: «حصان طروادة إسرائيلي».

Counterpunch,

<http://www.counterpunch.org/2008/09/27/an-israeli-trojanhorse>

جيمس بامفورد (3 أبريل 2012). مجلة وايرد. مقال: «شركات شبحية مرتبطة بإسرائيل تتجسس على أميركا لمصلحة إسرائيل».

Wired,

<http://www.wired.com/2012/04/shady-companies-nsa/all>.

ريتشارد ساندروز (ربيع 2012). موقع «برس فور كونفرسيشن». مقال: «شركات إسرائيلية جاسوسة: «فريت» و«ناروس»».

<http://coat.ncf.ca/P4C/66/spy.pdf>

79. في تسعينيات القرن العشرين، صدر عن «الأكاديميات الوطنية» التوصيات عينها: التوصية 1- يجب ألا يمنع أي قانون، صنع وبيع واستعمال أي نوع من التشفير داخل الولايات المتحدة. بصورة محدّدة، إنّ وجود حظر تشريعي على استعمال تشفير مؤتمن عند طرف ثالث، سيؤذي إلى إثارة مشاكل تقنية وقانونية ودستورية. تقنياً، هناك سبيل عدّة للاتفاف على حظر كذلك. وقانونياً، هناك مشكلات دستورية، خصوصاً ما تعلق بحرية التعبير، سوف تثار بشكل مؤكد؛ وهي مشكلات ليست هيئة الحل. صيغت التوصية كي تدعم على وجه الخصوص، ذلك الجانب من سياسة الإدارة بشأن كتابة التشفير. كنيث ديلو. دام وميربرت س. لين (1995): «مطبوعة الكليات الوطنية». كتاب: دور التشفير في حماية مجتمع المعلومات.

http://www.nap.edu/catalog.php?record_id=5131.

80. بروس شناير (4 أكتوبر 2014). شبكة «سي آن أن». مقال: «أوقفوا الهستيريا بشأن تشفير «آبل»».

CNN,

<http://edition.cnn.com/2014/10/03/opinion/schneier-apple-encryption-hysteria/index.html>

81. «المكتب التنفيذي للمحاكم الأمريكية» (11 يونيو 2014). تقرير: «الجدول 3: الاعتداءات الكبرى التي أوجبت إعطاء أذن قضائي بالتعرض، وفقاً لـ «يو إس سي» 2519»، من بداية يناير إلى نهاية ديسمبر للعام 2013. <http://www.uscourts.gov/Statistics/WiretapReports/wiretap-report-2013.aspx>.

82. آندي غرينبرغ (2 يوليو 2014). مجلة وايرد. «صعود ظاهرة التشفير، أدّى إلى تضليل الشرطة 9 مرات في 2013، وهو رقم قياسي».

Wired,

<http://www.wired.com/2014/07/rising-use-of-encryption-foiled-the-cops-a-record-9-times-in-2013>

83. ستيفن بلوفين (6-7 يونيو 2013). «مؤتمر قانوني الخصوصية»، بيركلي. ورقة بحث: «الاختراق الأخلاقي للكمبيوتر: استغلال الثغرات الموجودة في التنصت على الإنترنت».
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2312107
84. جاكوب آلباوم (23 أكتوبر 2013). صحيفة دير شبيغل. مقال: «برلين تشكو هل تجسست أميركا على هاتف المستشارة ميركل؟».
Der Spiegel,
<http://www.spiegel.de/international/world/merkel-calls-obama-over-suspicious-us-tappedher-mobile-phone-a-929642.html>
أيان ترانينور وفيليب أولترمان وبول لويس (23 أكتوبر 2013). صحيفة الغارديان. مقال: «أنفيلد ميركل تهاتف أوباما: هل تجسس على هاتف الخو؟».
85. إيوين ماكأسكل وجوليان بورغر (30 يونيو 2013). صحيفة الغارديان. مقال: «تسريبات جديدة عن وكالة الأمن القومي» تظهر تجسسها على حلفاء أوروبيين».
Guardian,
<http://www.theguardian.com/world/2013/oct/23/us-monitored-angelamerkel-german>.
- غلين غرينوالد (2014). كتاب لا مكان للاختباء: إدوارد سنودن و«وكالة الأمن القومي» وحال الرقابة في الولايات المتحدة. (دار ماكجيليان للنشر).
<http://leaksource.info/2014/07/31/glenn-greenwalds-no-place-to-hide-nsa-documents-excerpts>
86. لورا بواتراس ومارسيل روزنباخ وهولغر ستارك (26 أغسطس 2013). صحيفة دير شبيغل. مقال: «الاسم الشيفري هو «أبالاتشي»: كيف تجسست أميركا على أوروبا والأمم المتحدة».
Der Spiegel,
<http://www.spiegel.de/international/world/secret-nsa-documents-showhow-the-us-spies-on-europe-and-the-un-a-918625.html>
87. وجود حالات من عدم اليقين في المساحة بين الاستفادة والهجوم، قد يؤدي إلى تصاعد غير مرغوب فيه للتوتر. هربرت لين (خريف 2012). «دراسات استراتيجية». دراسة: «آليات تصعيد الصراع وإنهائه في الفضاء السبراني».
Strategic Studies Quarterly 6,
<http://www.au.af.mil/au/ssq/2012/fall/lin.pdf>.
88. بيتر كراسكا (يناير 2007). مجلة بوليس. مقال: «العسكرة وأعمال الشرطة: دلالتها بالنسبة لشرطة القرن 21».
Policing 1,
<http://cjmasters.eku.edu/sites/cjmasters.eku.edu/files/21stmilitarization.pdf>.
- آبغيل مال وكريستوفر كوينه (ربيع 2013). مجلة اندوبندنت ريفيو. تقرير: «عسكرة الشرطة المحلي في الولايات المتحدة».
17. *Independent Review*,
http://www.independent.org/pdf/tir/tir_17_04_01_hall.pdf
ماثيو ويتس (مارس 2013). مجلة دراسات 11/9. مقال: «أكثر تصميماً من أورويل: ظاهرة العسكرة الرديفة في الولايات المتحدة بعد 11/9».
36. *Journal of 9/11 Studies*,
<http://www.journalof911studies.com/resources/2013WittVol36Mar.pdf>
89. من الممكن البدء بقراءة كتاب جيد عن تلك المواضيع. راينيل بالكو (2013). بايليك أفيرز برس. «صعود الشرطة المحاربة: عسكرة قوات الشرطة الأمريكية».

<http://books.google.com/books?id=M3KSMQEACAAJ>

90. باراك أوباما (17 يناير 2014). صحيفة واشنطن بوست. مقال: «مقتطفات من خطاب الرئيس أوباما عن إصلاح وكالة الأمن القومي».

Washington Post,

http://www.washingtonpost.com/politics/full-text-of-president-obamas-jan-17-speech-on-nsa-reforms/2014/01/17/fa33590a-7f8c-11e3-9556-4a4bf7bcbdd84_story.html.

91. سكوت شارني (30 أبريل 2010). شركة مايكروسوفت. تقرير: «إعادة التفكير في التهديد السبراني: إطار للعمل والتحرك قديماً».

Microsoft Corporation,

<http://www.microsoft.com/en-us/download/details.aspx?id=747>

92. هناك كتابات عن إحماء الفاصل بين الجرائم وأعمال الحرب. بنجامين ب. بريستر (24 أغسطس 2007). كلية القانون في جامعة فلوريدا.

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1009845

93. بات كثيرون يستخدمون ذلك المصطلح المشحون بالمعاطف. ريتشارد بيهر (13 أكتوبر 2008). شبكة «فوكس نيوز». مقال: «أزمة غير مسبقة تضع «البنك الدولي» تحت حصار سبراني».

FOX News,

<http://www.foxnews.com/story/2008/10/13/world-bank-under-cyber-siege-in-unprecedented-crisis>.

مؤسسة «كاسبارسكي لاب» (2014). «مندی شركة كاسبرسكي للأمن الحكومي». تقرير: «ماذا تفعل أميركا إذا وقعت تحت حصار سبراني؟».

Kaspersky Government Cybersecurity Forum,

<http://kasperskygovforum.com>.

94. هناك اقتراح بإنشاء نوع من «التجنيد الإلزامي السبراني» بهدف تعبئة الشبكات في حال اندلاع حرب سبرانية. سوزان برنر وليو كلارك (أكتوبر 2010). «فاندربيلت جورنال أوف ترانزشونال لو». مقال: «المدنيون أثناء عمليات الحرب السبرانية: متطوعون».

Vanderbilt Journal of Transnational Law 43,

http://www.vanderbilt.edu/jotl/manage/wp-content/uploads/Brenner-Final_1.pdf.

95. «مؤسسة راند» (20 مارس 2001). تقرير: «عرض عام لـ «قانون بوزيه كوميتاتوس»».

http://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1251/MR1251.AppD.pdf

شارلز دويل وجنيفر إلسي (16 أغسطس 2012). خدمة بحوث الكونغرس. «عن «قانون بوزيه كوميتاتوس» وأمر متصلة به: استعمال العسكري لتنفيذ القانون المدني».

Congressional Research Service,

<http://www.fas.org/sgp/crs/natsec/R42659.pdf>

96. ريهت أ. هرمانديز (أكتوبر 2012). مجلة آر.مي. مقال: «عن «القيادة السبرانية الأمريكية»: الفضاء السبراني مساحة عمل لقوة أمريكية حاسمة».

Army,

<http://connection.ebscohost.com/c/articles/82115370/u-s-army-cyber-commandcyberspace-americas-force-decisive-action>.

97. في العقود الأخيرة، بذلت «وكالة الأمن القومي» جهداً أكبر في إمداد الشركات الأمريكية الخاصة بالبيانات، إضافة إلى حماية الاتصالات. تحتاج الشركات إلى عون الحكومة، لكنها تحتاج أن يجري ذلك بعلانية أكبر. سوزان لاندوا (29 سبتمبر 2014). «جورنال أوف ناشيونال سكيورتي لو أند بوليسي». مقال: «تحت الرادار: جهود «وكالة الأمن القومي» في حماية البنية التحتية للقطاع الخاص في الاتصالات».

Journal of National Security Law and Policy,

<http://jnsllp.com/2014/09/29/under-the-radar-nsas-efforts-to-secure-private-sector-telecommunications-infrastructure>

98. روبرت أ. روي (11 يونيو 1987). مجلس النواب، لجنة العلوم والفضاء والتكنولوجيا. مقال: «تقرير عن قانون أمن الكمبيوتر-1987».

<https://beta.congress.gov/congressional-report/107th-congress/senate-report/239/1>.

«مركز معلومات الخصوصية الإلكترونية» (2014). تقرير: «قانون أمن الكمبيوتر-1987».

<http://epic.org/crypto/csa>.

99. مولتن مولر (21 يونيو 2012). «مشروع حوكمة الإنترنت». تقرير: «تحليل المخاطر في المجلس العالمي للمعلوماتية والاتصالات» - القسم 4: «وحدة المعلوماتية والاتصالات والأمن السبراني».

Internet Governance Project,

<http://www.internetgovernance.org/2012/06/21/threat-analysis-of-the-wcit-4-cybersecurity>.

100. ذهبت حكومة البرازيل إلى حد اقتراح قانون بذلك الشأن، لكنه لم يقر. إستان إسرائيل وأنثوني بودل (28 أكتوبر 2013). وكالة رويترز للأنباء. مقال: «البرازيل تصرّ على تخزين بيانات الإنترنت محلياً، بعد انكشاف التجسس الأمريكي».

Reuters,

<http://www.reuters.com/article/2013/10/28/net-us-brazil-internet-idUSBRE99R10Q20131028>.

Anthony Boodle (18 Mar 2014), «Brazil to drop local data storage rule in Internet bill,

101. ميشال برينباوم (1 نوفمبر 2013). صحيفة واشنطن بوست. مقال: «ألمانيا تتطّلع لاحتفاظ ببيانات الإنترنت المحلي وبريدها الإلكتروني، داخل حدودها».

Washington Post,

http://www.washingtonpost.com/world/europe/germany-looks-at-keeping-its-internet-e-mail-traffic-inside-its-borders/2013/10/31/981104fe-424f-11e3-a751-f032898f2dbc_story.html.

102. شارلز ماينز (11 يوليو 2014). إذاعة دويتشه فيله. مقال: «روسيا تزيد صلابة الإنترنت بواسطة قانون الخوادم».

Deutsche Welle,

<http://www.dw.de/russia-tightensinternet-screws-with-server-law/a-17779072>

ادريان هيني (12 يوليو 2014). مجلة إيست-وست ديجيتال نيوز. مقال: «قوانين جديدة لتخزين المعلومات تؤثر في لاعبين محليين وأجانب- لكن لا يوجد «سور صيني» حول روسيا».

East-West Digital News,

<http://www.ewdn.com/2014/07/12/new-personal-data-storage-rules-to-affect-both-foreign-and-domestic-players-but-no-chinese-wall-surrounding-russia>

103. جاكلين بوركل (2 يناير 2014). مقال: «هل «فيسبوك» قضاء عام أو خاص؟».

<http://www.tandfonline.com/doi/abs/10.1080/1369118X.2013.870591>.

104. حتى لو فعلنا، لكننا وجدنا أنّها اتفاقية غائمة، وتعطي الشركة الحق في فعل ما يحلو لها... بل وتغير تلك الاتفاقية وفق إرادتها، من دون إشعارنا ولا الحصول على موافقتنا.

105. سكوت ليبارجر (1999). مقال: «قناة أم منتدى: مجازات قانونية من أجل الإنترنت».

<http://www.tandfonline.com/doi/abs/10.1080/08997225.1999.10556239>.

106. نواه د. زاتز (خريف 1998). مجلة هارفرد للقانون والتكنولوجيا. مقال: «أرصعة في الفضاء الافتراضي: إفساح المجال للمنتديات العامة في البيئة الإلكترونية».

12,

<http://jolt.law.harvard.edu/articles/pdf/v12/12HarvJLTech149.pdf>.

ليريسا ليدسكي (ديسمبر 2011). مجلة جامعة بوسطن للقانون. مقال: «منتدى عمومي 2.0».

<http://www.bu.edu/law/central/jd/organizations/journals/bulr/volume91n6/documents/LIDSKY.pdf>

الفصل 14: حلول للشركات

1. الأرجح أننا سنتمكن من ابتكار ما يخرجنا من الكارثة الإيكولوجية التي يمثلها التغير المناخي، وإن نحفظ بطريقتنا حاضراً في التعامل معها. بيورن لومبورغ (2001). «مطبعة جامعة كامبريدج». كتاب: البيئي المتشكك: قياس حال العالم فعلياً.

<https://encrypted.google.com/books?id=JuLko8USApwC>

2. «منظمة التنمية والتعاون الاقتصادي» (2013). وثيقة: «إطار الخصوصية- ومنظمة التنمية والتعاون الاقتصادي».

http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

3. البرلمان الأوروبي و«مجلس أوروبا» (24 أكتوبر 1995). وثيقة: «قانون من البرلمان الأوروبي ومجلس أوروبا» في 24 أكتوبر 1995، بشأن حماية الأفراد في ما يتصل بالتعامل مع المعلومات الشخصية والتحريك الحر لتلك المعلومات.

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML>

نيل روبنسون (2009). «مؤسسة راند». دراسة: «مراجعة القانون الأوروبي لحماية المعلومات».

RAND Corporation,

http://ico.org.uk/~media/documents/library/data_protection/detailed_specialist_guides/review_of_eu_dp_directive.ashx

4. كارلين ليلينغتون (14 مايو 2014). صحيفة أيريش تايمس. مقال: «تحليل: «غوغل» يتلقى ضربة جديدة بقوانين «الاتحاد الأوروبي» للخصوصية».

Irish Times,

<http://www.irishtimes.com/business/sectors/technology/analysis-google-takes-another-hit-with-eu-privacy-rulings-1.1793749>

«مؤسسة برايس ووتر هاوس كوبرز» (يوليو 2014). تقرير: «إصلاحات «الاتحاد الأوروبي» بشأن حماية البيانات: تحديثات للأعمال».

http://www.pwc.com/en_US/us/risk-assurance-services/publications/assets/pwc-eu-data-protection-reform.pdf.

5. المفوضية الأوروبية (25 يناير 2012). تقرير: «المفوضية تقترح إصلاحاً شاملاً لقوانين حماية الخصوصية».

http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm.

«المفوضية الأوروبية» (12 مارس 2014). تقرير: «التقدم في قانون «الاتحاد الأوروبي» لحماية البيانات الذي صار غير قابل للتراجع عنه، عقب تصويت في البرلمان الأوروبي».

http://europa.eu/rapid/press-release_MEMO-14-186_en.htm.

6. «منظمة التنمية والتعاون الاقتصادي» (2013). تقرير: «إطار الخصوصية في المنظمة».

http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

7. يصلح المقال التالي مدخلاً لفهم اقتصاديات خصوصية البيانات. تايلر مور (2011). منشورات «ناشيونال أكاديمي برس». مقال: «مدخل إلى اقتصاديات الأمن السراني: المبادئ وخيارات السياسة».

<http://cs.brown.edu/courses/csci1800/sources/lec27/Moore.pdf>.

8. تتزايد الاعتداءات والاختراقات بالنسبة لبيانات الرعاية الصحية أمريكياً، مع ما يرافق ذلك من غرامات. باتريك أوتول وكوري دنيس ودوغلاس ليفي (28 مارس 2014). مقال: «أفضل الممارسات لتجنب المسؤولية القانونية عن التعدي على البيانات».

<http://milawyersweekly.com/news/2014/03/28/commentarybest-practices-for-avoiding-data-breach-liability>

9. ساشا رومانوسكي وديفيد هوفمان واليساندرو أكويستي (25-26 يونيو 2012). «المنتدى السنوي اقتصاديات أمن المعلومات»، برلين (ألمانيا). دراسة: «تحليل تجريبي للمنازعات القضائية بشأن اختراق البيانات».

Annual Workshop on the Economics of Information Security, Berlin, Germany,

http://weis2012.econinfosec.org/papers/Romanosky_WEIS2012.pdf.

10. تدافع شركة «تارغت» عن نفسها في مجموعة دعاوى قضائية ترتبت على اختراق البيانات عندها في 2013. أليكس ويليامز (23 ديسمبر 2013). موقع «تيك كرانش». مقال: «ربما تغرم شركة «تارغت» 36 بليون دولار جزاء لاختراق بيانات بطاقات ائتمان لديها».

Tech Crunch,

<http://techcrunch.com/2013/12/23/target-may-be-liable-for-up-to-3-6-billion-from-creditcard-data-breach>

لانس ديروني (3 أبريل 2014). مقال: «المجلس القضائي للمنازعات المتعددة، يركز الدعاوى ضد «تارغت» في «منيسوتا»».

<http://www.law360.com/articles/524968/jpml-centralizetarget-data-breach-suits-in-minn>

11. برايان كرييس (8 يناير 2014). مدونة إلكترونية. مقال: «شركات تقاضي بنكاً بعد إفلاسها بسبب عملية سطو سبراني».

Krebs on Security,

<http://krebsonsecurity.com/2014/01/firm-bankrupted-by-cyberheist-sues-bank>

برايان كرييس (13 أغسطس 2014). مدونة إلكترونية. مقال: «شركة في ولاية «تينيسي» تقاضي بنكاً لتفريمه 37 ألف دولار، بعد عملية سطو سبراني».

Krebs on Security,

<http://krebsonsecurity.com/2014/08/tenn-utility-sues-bank-over-327k-cyberheist>

12. المقال التالي يحمل اقتراحاً بهذا الشأن. موريثيو نالدي ومارتا فلاميني وغويزيبي دا أكويستو (2013). مطبعة «سبرينغر». كتاب: الشبكة وأمن النظام. نص: «المسؤولية القانونية عن اختراق البيانات: اقتراح مقارنة تعتمد على ربط العقوبة بالدخل».

http://link.springer.com/chapter/10.1007%2F978-3-642-38631-2_20.

13. ويليس هير وآخرون (يوليو 1973). وزارة الصحة. تقرير: «سجلات، كومبيوترات وحقوق مواطنين: تقرير إلى اللجنة الاستشارية للوزير عن النظم المؤتمنة للمعلومات الشخصية».

US Department of Health, Education and Welfare,

<http://www.justice.gov/sites/default/files/opcl/docs/rec-com-rights.pdf>

14. كُتِبَ الكثير عن طرق استفادة قوانين الخصوصية من تشريعات البيئة. دينس د. هيرش (خريف 2006). مجلة جورجيا لوريفيو. مقال: «حماية البيئة الداخلية: ماذا تستطيع تشريعات الخصوصية تعلمه من قانون البيئة».

Georgia Law Review 41,

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1021623

إيرا س. روبنشتاين (2011). دراسة: «الخصوصية والابتكار التشريعي: الخروج من الأعراف الطوعية».

http://www.ftc.gov/sites/default/files/documents/public_comments/privacy-roundtables-comment-projectno.p095416-544506-00022/544506-00022.pdf.

15. ربما برزت الحاجة إلى شيء من الاستثناءات للبرمجيات المجانية والمفتوحة المصدر، وكذلك الحالات التي لم يوقع المستخدم فيها عقداً مع الشركة البائعة للبرمجيات.
16. غويسبي داري-ماتياشي ونوينو غاروبا (مايو 2009). مجلة جورنال أوف لو، أيكونوميكس أند أورغنايزيشن. مقال: «التجنب الأقل كلفة: مسألة الأمان العام».
Journal of Law, Economics, and Organization 25,
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=560062.
بول روزنزفايغ (5 نوفمبر 2013). مجلة لوفير. مقال: «الأمن السبراني والتجنب بالكلفة الأقل».
Lawfare,
<http://www.lawfareblog.com/2013/11/cybersecurity-and-the-least-costavoider>
17. الحق أن مفهوم ملكية البيانات معقد تماماً. علي الخوري (نوفمبر 2012). مقال: «ملكية المعلومات: من يملك «بياناتي»؟».
<http://www.id.gov.ae/assets/FNukwmhbQ4k.pdf.aspx>
جاكوب فيكتور (نوفمبر 2013). تقرير: «قانون الاتحاد الأوروبي» عن حماية البيانات العامة: نحو نظام مناسب في حماية خصوصية المعلومات».
<http://www.yalelawjournal.org/comment/the-eu-general-data-protection-regulation-toward-a-property-regime-for-protecting-data-privacy>
18. جنيفر فالنتينو-دي فرايز وجيرمي سينغر-فاين (7 ديسمبر 2012). صحيفة وول ستريت جورنال. مقال: «إنهم يعرفون ماذا تتسوقون».
Wall Street Journal,
<http://online.wsj.com/news/articles/SB10001424127887324784404578143144132736214>
جيرمي سينغر-فاين (7 ديسمبر 2012). صحيفة وول ستريت جورنال. مقال: «كيف تراقبك «داتايوم»».
<http://blogs.wsj.com/digits/2012/12/07/how-dataium-watches-you>
19. فرانك باسكال (21 أبريل 2009). مقال: «الميل المقلق صوب تبني نظم التصنيف المستندة إلى السرية التجارية».
<http://www.chicagoip.com/pasquale.pdf>
20. إيثان زوكرمان (5 سبتمبر 2012). مقال: «لوائح إدارة أمن النقل» للتدقيق قبل السفر بين العدالة وضبابية الخوارزميات».
21. دانيال فايتزنر (-29 30 يناير 2014). «المنتدى الثاني في «ماساشوستس-كامبردج» عن الموثوقية: سياسة العلوم والتكنولوجيا». دراسة: «فلسفة القانون في الموثوقية».
2nd International Workshop on Accountability: Science, Technology and Policy, Cambridge, Massachusetts,
<http://dig.csail.mit.edu/2014/AccountableSystems2014/abs/weitzner-account-jurisprudence-abs.pdf>
إد فيلتن (12 سبتمبر 2012). موقع «فريدوم تو تينكر». مقال: «الخوارزميات الموثوقة».
Freedom to Tinker,
<https://freedom-to-tinker.com/blog/felten/accountable-algorithms>
22. تشمل الأمثلة على ذلك شركة «مايكروسوفت» و«المنتدى الاقتصادي العالمي». كريغ موندي (مارس / أبريل 2014). مجلة فورين أفييرز. مقال: «البراماتية في الخصوصية: ركز على استعمال المعلومات وليس تجميعها».
Foreign Affairs 93,
<http://www.foreignaffairs.com/articles/140741/craig-mundie/privacy-pragmatism>
ويليام هوفمان (مايو 2014). «المنتدى الاقتصادي العالمي». تقرير: «إعادة التفكير في المعلومات الشخصية: نظرة جديدة لمتين الثقة».
World Economic Forum,
<http://reports.weforum.org/rethinking-personal-data>

فريد كاي وبيتر كولين وفينكتور ماير- شوينرغر (مايو 2014). «معهد أكسفورد للإنترنت» في جامعة أكسفورد. دراسة: «مبادئ حماية المعلومات في القرن 21: إعادة النظر في الخطوط التوجيهية لمنظمة التنمية والتعاون الاقتصادي»-1980.

Oxford Internet Institute, University of Oxford,
http://www.oii.ox.ac.uk/publications/Data_Protection_Principles_for_the_21st_Century.pdf

«مجلس مستشاري الرئيس عن العلوم والتكنولوجيا» (مايو 2014). تقرير: «البيانات الضخمة» والخصوصية: مقارنة تكنولوجية.

http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf.

23. كريس غاي هوفناغل (2 سبتمبر 2014). موقع «سلايت». مقال: «المخادعة الإيحائية في الخصوصية البراغمية».

Slate,
http://www.slate.com/articles/technology/future_tense/2014/09/data_use_regulation_the_libertarian_push_behind_a_new_take_on_privacy.single.html

24. أ. ميخائيل فرومكين (23 فبراير 2014). جامعة ميامي. دراسة: «تنظيم الرقابة العامة بوصفها تلويناً للخصوصية: دروس من القوانين عن الأثر البيئي».

University of Miami,
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2400736

25. جولي بريل (2 يونيو 2014). «ورشة مستشاري الاتحاد الأوروبي» لحماية المعلومات عن «حماية المستهلك والمنافسة في العصر الرقمي»، بروكسل، بلجيكا. دراسة: «نسخ مفرض مركز لحماية الخصوصية والمنافسة في عصر البيانات الضخمة».

http://www.ftc.gov/system/files/documents/public_statements/313311/140602edpsbrill2.pdf.

جولز بولونتسكي وعمر تينه (6 ديسمبر 2012). «فيوتشر برايفسي فوروم». تقرير: «ليست المسألة حجم البيانات التي تحوزها، بل طريقة استعمالك لها».

Future of Privacy Forum,
http://www.futureofprivacy.org/wp-content/uploads/FPF-White-Paper-Its-Not-How-Much-Data-You-Have-But-How-You-Use-It_FINAL.pdf

26. «الاتحاد الأوروبي» (9 ديسمبر 2013). وثيقة: «السلطات الوطنية لحماية البيانات».

http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm

27. آلون هاليفي وبيتر نورفيج وفرناندو بيريرا (مارس/أبريل 2009). «معهد المهندسين الكهربائيين والإلكترونيين: النظم الذكية 2.0». «الكفاءة غير المنطقية للبيانات».

https://static.googleusercontent.com/media/research.google.com/en/us/pubs/archive/35179.pdf

28. دووغ غروس (7 يناير 2013). شبكة «سي أن أن». مقال: «مكتبة الكونغرس» تنقّب في 170 بليون تغريدة. CNN,
http://www.cnn.com/2013/01/07/tech/social-media/library-congress-twitter.

29. مارتن فاو (12 ديسمبر 2013). «داتنشايرشزامكايت».

http://martinfowler.com/bliki/Datensparsamkeit.html.

30. بالطبع، الحميات القانونية لا تتحوّل بالضرورة إلى حماية حقيقية. في 2011، اكتُشف أن الحكومة الألمانية تتجسّس على مواطنيها باستخدام برنامج خبيث من نوع «تروجان»، مخترقة بنفسها قوانينها القوية في حماية البيانات. وكما علمنا مراراً وتكراراً، لا قانون بإمكانه أن يحمينا من حكومة ترفض الالتزام به. «نادي فوضى الكمبيوتر» (8 أكتوبر 2011). تقرير: «تحليل «نادي فوضى الكمبيوتر» لبرنامج حكومي خبيث».

Chaos Computer Club analyzeshowgovernment malware.,
http://ccc.de/en/updates/2011/staatstrojaner

31. دي. آل. إيه باير (7 مارس 2013). دراسة «قوانين حماية البيانات في العالم». http://files.dlapiper.com/files/Uploads/Documents/Data_Protection_Laws_of_the_World_2013.pdf
ثيودور كوبوس الثالث وغونزالو زيبالوس (19 فبراير 2014). موقع «بايكر هوستلر». دراسة: «الوجيز العالمي في قوانين حماية خصوصية البيانات في 2014».
- Baker Hostetler,
<http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/International-Compendium-of-Data-Privacy-Laws.pdf>.
32. أستطيع الوصول إلى بعضها إذا فعلت خاصية التسجيل الزمني للبحث. دايف غرينباوم (12 يوليو 2014). موقع «لايف هاكلر». مقال: «أضاف «غوغل» صفحة لتاريخ عمليات البحث، تساعد على مزيد من التحكم ببياناتك».
- Life Hacker,
<http://lifelifehacker.com/googles-newaccount-history-page-helps-further-control-1603125500>
33. هيو كامبوس (19 نوفمبر 2011). مدونة إلكترونية. «هيو كامبوس يقاتل من أجل حقه في النفاذ إلى معلومات عن قلبه».
- <http://tedxtalks.ted.com/video/TEDxCambridge-Hugo-Campos-fight>
34. بروس شناير (يوليو / أغسطس). مقال: «تصنيف لبيانات الدسوشال ميديا».
- http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5523874.
35. بلايك روز (13 سبتمبر 2011). موقع «فيسبوك». توجيه: «قائمة أصدقاء محسنة».
- Facebook,
<https://www.facebook.com/notes/facebook/improvedfriend-lists/10150278932602131>
36. توني برادي (13 أكتوبر 2010). مجلة عالم الكمبيوتر. مقال: «أنظن أن تغريداتك خصوصية؟ فخر ثانية».
- PC World,
http://www.pcworld.com/article/207710/think_your_twitter_dm_is_private_think_again.html
37. ليسلي ميرديث (15 يناير 2013). شبكة «أن بي سي نيوز». مقال: «لماذا يجب عليك جعل حسابك على «أنستغرام» خصوصياً قبل يوم السبت؟».
- NBC News,
<http://www.nbcnews.com/tech/internet/why-you-should-make-instagram-private-saturday-f1B7987618>
38. سرجي مالينكوفيتش. صحيفة مختبر كاسبارسكي. مقال: «كيف تحمي خصوصيتك على «بينترست»».
- Kaspersky Lab Daily,
<http://blog.kaspersky.com/protect-your-privacy-on-pinterest>.
39. «المكتب التنفيذي للرئاسة» (1 مايو 2014). تقرير: «البيانات الضخمة: النقاط الفرصة والحفاظ على القيم».
- http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.
40. يارون لانير (2013). دار «ساميون وشوستر». كتاب: «من يملك المستقبل؟»
- Simon and Schuster,
<http://books.google.com/books?id=wLobtmRYmQC>
41. «المكتب التنفيذي للرئاسة» (فبراير 2012). تقرير: «خصوصية بيانات المستهلك في عالم مترابط بالشبكات: إطار عمل لحماية الخصوصية وتحفيز الابتكار في الاقتصاد الرقمي العالمي».
- <http://www.whitehouse.gov/sites/default/files/privacy-final.pdf>.
42. المفوضية الأوروبية (8 يوليو 2014). تقرير: «ورقة الحقائق عن تشريع «الحق في النسيان»».

http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf

43. روري سيلان- جونز (13 مايو 2014). هيئة الإنعاط البريطانية. مقال: «المحكمة الأوروبية تؤيد الحق في النسيان» في قضايا مرفوعة ضد «غوغل».

BBC News,

<http://www.bbc.com/news/world-europe-27388289>.

44. جاين ويكفيلد (15 مايو 2014). هيئة الإنعاط البريطانية. مقال: «سياسيون ومحبو جنس الأطفال يطلبون من «غوغل» أن «يجري نسيانهم»».

BBC News,

<http://www.bbc.com/news/technology-27423527>.

45. أليساندرو مانتيليريو (يونيو 2013). تقرير: «اقتراح الاتحاد الأوروبي» بصدد قانون عام لحماية البيانات، وجذور «الحق في النسيان».

<http://www.sciencedirect.com/science/article/pii/S0267364913000654>.

46. أجريت تجارب عدة للبرهان على ذلك. باتريسيا نوربرغ ودانيال ر. هورني وديفيد أ. هورني (صيف 2007). مجلة جورنال أوف كونسيومر آفيرز. دراسة: «مفارقة الخصوصية: نوايا الكشف عن المعلومات الشخصية مقابل السلوكيات».

Journal of Consumer Affairs 41,

<http://onlinelibrary.wiley.com/doi/10.1111/j.1745-6606.2006.00070.x/abstract>

سوزان ووترز وجيمس أكرمان (أكتوبر 2011). مجلة جورنال أوف كومبيوتر ميديتد كومونيكايشنز. دراسة: «استكشاف الخصوصية وإدارتها في «فيسبوك»: الدوافع والنتائج المتصورة المتصلة بإشهار المعلومات طوعياً».

Journal of Computer-Mediated Communication 17,

<http://onlinelibrary.wiley.com/doi/10.1111/j.1083-6101.2011.01559.x/full>

أليساندرو أكويستي، رالف كروس وفريد شتوتزمان (أبريل 2013). مجلة جورنال أوف برايفسي أند كونفيدينشاليتي. دراسة: «المُصغون الصامتون: تطوّر الخصوصية والإشهار على «فيسبوك»».

Facebook, *Journal of Privacy and Confidentiality* 4,

https://www.cylab.cmu.edu/news_events/news/2013/acquisti-7-year-study-facebook-privacy.html

47. تبين أنه من السهولة بمكان التلاعب بالناس كي ينسوا قلقهم بشأن الخصوصية. إدريس ادجيريد وآخرون (22 مارس 2013). دراسة: «براعات الخصوصية: التأطير، الكشوفات، وحدود الشفافية».

<http://www.heinz.cmu.edu/~acquisti/papers/acquisti-sleights-privacy.pdf>.

48. سارة م. واتسون (29 أبريل 2014). مقال: «إذا عرف المستهلكون كيف يستعملون بياناتهم، كيف يدعونها مربية بعد ذلك؟».

<http://blogs.hbr.org/2014/04/if-customers-knew-how-you-use-their-data-would-theycall-it-creepy>.

49. كريس جاي هوفناغل وجان هافنغتون (28 فبراير 2014). مجلة لو ريفيو- جامعة كاليفورنيا. دراسة: «المجاني: جردة حساب لتكاليف السعر الأكثر شعبية على الإنترنت».

UCLA Law Review 61,

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2235962.

50. كريستن مارتين (2 ديسمبر 2013). مقال: «تكاليف التعاملات، الخصوصية، والثقة: الأهداف الحميدة والسقوط المتوقع لسياسة الإشعار وخيار احترام الخصوصية على الإنترنت».

<http://firstmonday.org/ojs/index.php/fm/article/view/4838/3802>.

51. الأقرب إلى ما أعرف، أن تلك الفكرة اقترحها أستاذ حقوق بشكل مستقل. جيري كانغ (مارس 2012). بحث: «خصوصية الرقابة الذاتية».

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1729332.

- جاك م. بالكين (5 مارس 2014). بحث: «المرجعيات الموثوقة معلوماتياً في العصر الرقمي».
<http://balkin.blogspot.co.uk/2014/03/informationfiduciaries-in-digital-age.html>.
52. جوناثان زيترتين (1 يونيو 2014). موقع «نيو ريپابلِك». مقال: «يستطيع «فيسبوك» أن يحسم الانتخابات من دون أن يلاحظه أحد».
- New Republic*,
<http://www.newrepublic.com/article/117878/information-fiduciary-solution-facebook-digital-gerrymandering>
53. دان غير (9 أكتوبر 2013). «مبادلات في الأمن السبراني».
<http://geer.tinho.net/geer.uncc.9x13.txt>
54. اعتذر مبتكر الإعلانات الصغيرة التي تقفز على شاشة الحاسوب من دون استئذان [«بوب اب آدس»] عما فعله. إيثان زوكerman (14 أغسطس 2014). مجلة «آتلانتيك». مقال: «الخطيئة الأصلية للإنترنت».
- Atlantic*,
<http://www.theatlantic.com/technology/archive/2014/08/advertising-is-the-internets-original-sin/376041>.
55. آن كافوكيان (يناير 2011). مقال: «الخصوصية بالتصميم: المبادئ التأسيسية السبعة».
<http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf>.
- «لجنة التجارة الفيدرالية» (مارس 2012). تقرير: «حماية خصوصية المستهلك في زمن التغير السريع: توصيات إلى رجال الأعمال وصنّاع السياسة».
- <http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>.
56. أنغريد لوندين (30 سبتمبر 2013). موقع «تيك كرانش». تقرير: «تشكل الإعلانات الرقمية 22 % من إجمالي إنفاق أميركا على الإعلانات في 2013، وإعلانات الهواتف النقّالة 3.7 %، فيما الإتفاق العالمي على الإعلانات يقارب 503 بليون دولار».
- Tech Crunch*,
<http://techcrunch.com/2013/09/30/digital-ads-will-be-22-of-all-u-s-ad-spend-in-2013-mobile-ads-3-7-total-gobal-ad-spend-in-2013-503b-sayszenithoptimedia>
- الرسوم البيانية للتسويق (23 ديسمبر 2013). تقرير: «الغوص في البيانات: عن تأثير الإعلانات التلفزيونية في الولايات المتحدة».
- <http://www.marketingcharts.com/wp/television/data-dive-us-tv-ad-spend-and-influence-22524>.
57. جيمس كانستلر (21 أكتوبر 2005). موقع «رايز زي هامر». مقال: «سيكولوجية الاستثمار السابق».
<http://www.raisethehammer.org/article/181>.
58. شارلي سافاج (14 مايو 2014). صحيفة نيويورك تايمس. مقال: «وفق أوراق كُشِفَتْ أخيراً، شركات للهواتف قاومت «وكالة الأمن القومي» في المحاكم».
- New York Times*,
<http://www.nytimes.com/2014/05/15/us/politics/phone-company-pushed-back-against-nsasdata-collection-court-papers-show.html>
- كلير كاين ميللر (13 يونيو 2013). صحيفة نيويورك تايمس. مقال: «قرار سري لحكمة يضع شركات التكنولوجيا في قيود البيانات».
- New York Times*,
<http://www.nytimes.com/2013/06/14/technology/secret-court-ruling-put-tech-companies-in-databind.html>.

59. إيوين ماكأسكل (9 سبتمبر 2013). صحيفة الغارديان. مقال: «قضية من «ياهو» ضد طلبات «وكالة الأمن القومي» لبيانات المستخدم».

Guardian,

<http://www.theguardian.com/world/2013/sep/09/yahoo-lawsuit-nsa-surveillance-requests>

مايك مازنيك (27 يناير 2014). موقع «تيك ديرت». مقال: «تسوية بين السلطات الفيدرالية وشركات الإنترنت تقضي بأن لا تسلم الأخيرة إلا أقل مما يكفي من المعلومات عن جهود الرقابة».

Tech Dirt,

<https://www.techdirt.com/articles/20140127/17253826014/feds-reach-settlement-with-internet-companiesallowing-them-to-report-not-nearly-enough-details-surveillance-efforts.shtml>.

سبنسر إكرمان (3 فبراير 2014). صحيفة الغارديان. مقال: «مايكروسوفت، «فيسبوك»، «غوغل»، و«ياهو» تنشر طلبات أرسلتها «وكالة الأمن القومي»».

Guardian,

<http://www.theguardian.com/world/2014/feb/03/microsoft-facebook-google-yahoo-fisa-surveillance-requests>

60. «غوغل» (2014). «تقرير الشفافية».

<https://www.google.com/transparencyreport/userdatarequests/US>.

61. برايان فانغ (9 يناير 2014). صحيفة واشنطن بوست. مقال: «أول شركة اتصالات هاتفية تنشر تقرير شفافية، لم تكن «إيه تي أند تي» أو «فريزون»».

Washington Post,

<http://www.washingtonpost.com/blogs/the-switch/wp/2014/01/09/the-first-phonecompany-to-publish-a-transparency-report-isnt-att-or-verizon>.

62. «فريزون» (22 يناير 2014). «تقرير شفافية من «فريزون»».

<http://transparency.verizon.com/us-data>.

63. غلين غرينوالد (5 يونيو 2013). صحيفة الغارديان. «تجمع «وكالة الأمن القومي» سجلات هواتف الملايين من زبائن شركة «فريزون» يوميًا».

Guardian,

<http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order>

64. كريغ تيمبرغ (1 مايو 2014). صحيفة واشنطن بوست. مقال: «آبل»، «فيسبوك»، وغيرهما تتحدى الحكومة بإبلاغ المستخدم عن طلبات سرية للبيانات».

http://www.washingtonpost.com/business/technology/apple-facebook-others-defyauthorities-increasingly-notify-users-of-secret-data-demands-after-snowden-revelations/2014/05/01/b41539c6-cfd1-11e3-b812-0c92213941f4_story.html

65. جاكوب سيفال (30 أغسطس 2013). مقال: «مايكروسوفت» و«غوغل» تتحالفان لمقاضاة الحكومة الفيدرالية بشأن تجسس «وكالة الأمن القومي»».

<http://bgr.com/2013/08/30/microsoft-google-nsa-lawsuit>.

66. إيوين ماكأسكل (9 سبتمبر 2013). صحيفة الغارديان. مقال: «قضية من «ياهو» ضد طلبات «وكالة الأمن القومي» لبيانات المستخدم».

Guardian,

<http://www.theguardian.com/world/2013/sep/09/yahoo-lawsuit-nsa-surveillance-requests>

كريغ تيمبرغ (11 سبتمبر 2013). صحيفة واشنطن بوست. مقال: «الحكومة الأميركية هددت بفرض غرامات ضخمة ما لم يعطها «ياهو» بياناته».

Washington Post,

http://www.washingtonpost.com/business/technology/us-threatened-massive-fine-to-force-yahoo-to-release-data/2014/09/11/38a7f69e-39e8-11e4-9c9f-ebb47272e40e_story.html.

67. سايبوس فاريفار (5 نوفمبر 2013). موقع «أرس تكنيكا» مقال: «في موقف صلب حيال الخصوصية، «أبل» تنشر تقارير نادرة عن «عصافير المذكرات».

Ars Technica,

<http://arstechnica.com/tech-policy/2013/11/apple-takes-strong-privacy-stance-in-new-report-publishes-rare-warrant-canary>

68. في الواقع، اختفت «عصافير المذكرات» من تقارير «أبل» التي تلت التقرير الذي أطلق تلك العبارة. ولا يعرف أحد ما المقصود من تلك العبارة على وجه التحديد. جيف جون روبرتس (18 سبتمبر 2014). مقال: «اختفاء «عصافير المذكرات» من تقارير «أبل»، ما يوحي بضغط متزايدة بقانون باتريوت».

<https://gigaom.com/2014/09/18/apples-warrant-canary-disappears-suggesting-new-patriot-act-demands>.

69. تحتفظ «مؤسسة الحدود الإلكترونية» بالسجل القياسي في ذلك المجال. نايت كاردوزو وباركر هيفنز وكيرت أوبسامل (13 مارس 2014) تقرير: «تحديث: تشفير التقرير عن الدويب»: من يفعل ماذا.

<https://www.eff.org/deeplinks/2013/11/encrypt-web-report-whos-doing-what>

70. شون غالاهاو (6 نوفمبر 2013). موقع «أرس تكنيكا». مقال: «تقنيو «غوغل» يقبلون ظهور المجن لدوكالة الأمن القومي»، ويشفرون شبكته الداخلية.

Ars Technica,

<http://arstechnica.com/information-technology/2013/11/googlers-say-f-you-to-nsa-company-encrypts-internal-network>.

71. بارتون غيلمان وأشكان سلطاني (14 أكتوبر 2013). صحيفة واشنطن بوست. مقال: «تجمع «وكالة الأمن القومي» ملايين دفاتر المناوين في البريد الإلكتروني عالمياً».

Washington Post,

http://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-email-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story.html

72. اندريا بيترسون وبارتون غيلمان وأشكان سلطاني (14 أكتوبر 2013). صحيفة واشنطن بوست. مقال: «أخيراً، «ياهو» يعتمد بروتوكول «إس إس أل» في بريد مستخدميه على الدويب».

Washington Post,

<http://www.washingtonpost.com/blogs/the-switch/wp/2013/10/14/yahooto-make-ssl-encryption-the-default-for-webmail-users-finally>.

73. كريغ تيمبرغ وبارتون غيلمان وأشكان سلطاني (26 نوفمبر 2013). صحيفة واشنطن بوست. مقال: «بعد ارتياها في تجسس «وكالة الأمن القومي» عليها، «مايكروسوفت» تشرع جهود تشفير الحراك الإلكتروني على الإنترنت».

Washington Post,

http://www.washingtonpost.com/business/technology/microsoft-suspecting-nsa-spying-to-ramp-up-efforts-to-encrypt-its-internet-traffic/2013/11/26/44236b48-56a9-11e3-8304-caf30787c0a9_story.html

74. هناك أمثلة عدة. داني ياردون (3 يونيو 2014). صحيفة وول ستريت جورنال. مقال: «شركة «كومكاست» تشفير البريد الإلكتروني توجهاً للأمن».

Wall Street Journal,

<http://online.wsj.com/articles/comcast-to-encrypt-email-for-security-1401841512>.

مايك كامبل (13 يونيو 2014). موقع «أبل إنسايدر». مقال: «شركة «أبل» تسعى لتشفير الإيميل في «آي كلاود»، أثناء تنقله بين مقدمي خدمة الإنترنت».

Apple Insider,

<http://appleinsider.com/articles/14/06/13/apple-will-soon-encrypt-icloud-emails-in-transit-between-service-providers->

75. نايت كاردوزو وباركر ميغنز وكيت أوبسامل (13 مارس 2014) تقرير: «تحديث: تشفير التقرير عن الدويب: من يفعل ماذا».

<https://www.eff.org/deeplinks/2013/11/encrypt-web-report-whos-doing-what>

كلير كاين ميللر (13 يونيو 2013). صحيفة نيويورك تايمس. مقال: «قرار سري لمحكمة يضع شركات التكنولوجيا في قيود البيانات».

New York Times,

<http://www.nytimes.com/2013/06/14/technology/secret-court-ruling-put-tech-companies-in-databind.html>.

76. في أواخر 2014، عدلت «أبل» نظام عملها، فبات كل شيء لديها مشفراً. وتحتوي هواتف الدأندرويد، مزايا تشفيرية منذ 2011، لكن «غوغل» لم يعتمدها كأساس لأعمال تلك الهواتف إلا في 2014، كي ينافس «أبل». ديفيد سانغر وبرايان شين (26 سبتمبر 2014). صحيفة نيويورك تايمس. مقال: «بداية حقبة ما بعد سونودن: هواتف «آي فون» تغلق أبوابها بوجه «وكالة الأمن القومي»».

New York Times,

<http://www.nytimes.com/2014/09/27/technology/iphone-locks-out-the-nsa-signaling-a-post-snowden-era-.html>

77. «غوغل» (3 يونيو 2014). المدونة الإلكترونية الرسمية لـ«غوغل». وثيقة: «تقرير الشفافية: حماية الإيميل أثناء ترحاله في الإنترنت».

Google Official Blog,

<http://googleblog.blogspot.com/2014/06/transparency-report-protecting-emails.html>

78. كلير كاين ميللر (13 يونيو 2013). صحيفة نيويورك تايمس. مقال: «قرار سري لمحكمة يضع شركات التكنولوجيا في قيود البيانات».

New York Times,

<http://www.nytimes.com/2013/06/14/technology/secret-court-ruling-put-tech-companies-in-databind.html>.

كريغ تيمبرغ (11 سبتمبر 201). صحيفة واشنطن بوست. مقال: «الحكومة الأميركية حددت بقرض غرامات ضخمة ما لم يعطها «ياهو» بياناته».

Washington Post,

http://www.washingtonpost.com/business/technology/us-threatened-massive-fine-to-force-yahoo-to-release-data/2014/09/11/38a7f69e-39e8-11e4-9c9f-ebb47272e40e_story.html.

79. كيم زيتر (28 أغسطس 2012). مجلة وايرد. مقال: «معركة «تويتر» دفاعاً عن نشطاء حركة «احتلوا وول ستريت»».

Wired,

<http://www.wired.com/2012/08/twitter-appeals-occupy-order>.

تيفاني كاري (14 سبتمبر 2012). شبكة «بلومبرغ نيوز». مقال: «تحت ختم رسمي، «تويتر» يسلم تقريرات نشطاء حركة «احتلوا وول ستريت»».

Bloomberg News,

<http://www.bloomberg.com/news/2012-09-14/twitter-turns-over-wall-street-protester-posts-under-seal.html>

80. فينديو غويل وجيمس س. ماكيني جونور (26 يونيو 2014). صحيفة نيويورك تايمس. مقال: «بعد إرغامه على تسليم بيانات، «فيسبوك» يرفع دعوى قضائية».

81. تبنت 3 منظمات أهلية قضية «لافايت» ضد الداف بي آي»، واستطاعت أن تتخذ موقف «صديق المحكمة»، بمعنى أن تكون مستشارة بشكل موثوق في قضية ليست طرفاً فيها، ولا مصلحة مباشرة لها منها. كانت

- تلك المنظمات الثلاث هي: «مؤسسة الحدود الإلكترونية» (*Electronic Frontier Foundation*) المعروفة باسمها المختصر «إي إف إف» (*EFF*) و«الاتحاد الأمريكي للحريات المدنية» (*American Civil Liberties Union*) المعروفة باسمها المختصر «إيه سي آل يو» (*ACLU*)، و«الشركة للمسؤولية المحدودة المؤيدة شعبياً» (*Empeopled Limited Liability Company*). وتوجد تفاصيل تلك القضايا الثلاث التي رفعت كلها بتاريخ (25 أكتوبر 2013)، على المواقع الإلكترونية للمنظمات الثلاث على الإنترنت.
82. ريببكا ماكينون (2006). منظمة «هيومن رايتس ووتش». تقرير: «السباق إلى الهاوية: تواطؤ الشركات في الحجب الصيني للإنترنت».
- Human Rights Watch,
<http://www.hrw.org/reports/2006/china0806/5.htm>
83. توماس لي (25 مايو 2014). صحيفة سان فرانسيسكو كرونكل. مقال: «نتبه إلى عملك: شركات التقنية تتلصق في استخدام عضلاتها».
- San Francisco Chronicle*,
<http://www.sfgate.com/technology/article/Mind-Your-Business-Slow-flex-of-tech-s-lobbying-5504172.php>.
- جوزيف بمن (5 يونيو 2014). وكالة «رويترز» للأنباء. مقال: «شركات التكنولوجيا الأمريكية تعزز أمن المعلومات لخلق التجسس العام».
- Reuters,
<http://www.reuters.com/article/2014/06/05/us-cybersecurity-tech-idUSKBN0EG2BN20140605>.
- Reform Government Surveillance (2014),
<https://www.reformgovernmentsurveillance.com>
84. زاك ويتكر (4 شباط 2013). شبكة «زد نت». مقال: «مجموعات الدفاع عن الخصوصية تناشد الحكومة الأمريكية التوقف عن ممارسة ضغوط ضد إصلاح قانون البيانات في الاتحاد الأوروبي».
- ZDNet,
<http://www.zdnet.com/privacy-groups-call-on-us-government-to-stop-lobbyingagainst-eu-data-law-changes-7000010721>.
- ديفيد ماير (12 مارس 2014). موقع شركة «جيجاوم». مقال: «شركات الدوبي» تواجه مجموعة جديدة من القوانين الصارمة بشأن الخصوصية في أوروبا: إليكم ما يجب توقعه».
- Gigaom,
<http://gigaom.com/2014/03/12/web-firms-face-a-strict-new-set-of-privacy-rules-in-europe-heres-what-to-expect>.
85. تيم بيرنرز-لي (ديسمبر 2010). مجلة ساينتفك أميركان. مقال: «يحيى الدوبي».
- Scientific American,
http://www.cs.virginia.edu/~robins/Long_Live_the_Web.pdf.
86. جيسا كيس (11 مارس 2014). صحيفة الغارديان. مقال: «نحو «ماغنا كارتا» للإنترنت: بيرنرز-لي يدعو إلى وثيقة حقوق للدوبي».
- Guardian,
<http://www.theguardian.com/technology/2014/mar/12/online-magna-carta-berners-lee-web>.
87. توماس هوبز (1651). دار «أندرو كوكس». كتاب: ليفياتان.
- <http://www.gutenberg.org/files/3207/3207-h/3207-h.htm>
88. جون لوك (1690). دار «أونشام تشرشل». كتاب: مبحثان للحكم.
- <http://books.google.com/books/?id=LqA4nQEACAAJ>.

89. الصوت العام (3 نوفمبر 2009). «إعلان مدريد للخصوصية» (2009). المؤتمر الدولي لمفوضي الخصوصية وحماية البيانات، مدريد، إسبانيا.
http://privacyconference2011.org/htmls/adoptedResolutions/2009_Madrid/2009_M1.2.pdf
90. ربيكا ماكينون (2012). كتاب: موافقة المتصلين بالشبكات.
http://www.owlasylum.net/owl_underground/social/ConsentoftheNetworked.pdf.

الفصل 15: حلول للبقية منا

1. إيبين موغلن (27 مايو 2014). صحيفة الغارديان. مقال: «الخصوصية تتعرض للهجوم: وثائق وكالة الأمن القومي» تكشف تهديدات جديدة للديمقراطية.
Guardian,
<http://www.theguardian.com/technology/2014/may/27/-sp-privacy-under-attack-nsa-files-revealed-new-threats-democracy>.
2. وضع عالم الاجتماع غاري ماركس تصنيفاً يتضمّن 14 طريقة تمكّن الناس من مقاومة الرقابة؛ واعتمدت على تصنيفه في هذا الفصل. غاري ت. ماركس (مايو 2003). مجلة جورنال أوف سوشال إيشوز. بحث: «ضربة على الحذاء: ملاحظة الرقابة الجديدة ومقاومتها».
<http://web.mit.edu/gtmrx/www/tack.html>
3. آر. جاسون كرونك (25 نوفمبر 2013). موقع «برايفسي مافريك». مقال: «أفكار حول عبارة «تقنيات تعزيز الخصوصية»».
Privacy Maverick,
<http://privacymaverick.com/2013/11/25/thoughts-on-the-term-privacy-enhancing-technologies>.
4. جون برودكين (2 مايو 2014). موقع «أرس تكنيكا». مقال: «مكوّن إلكتروني للاتصال بالإنترنت صنعتها «مؤسسة الحدود الإلكترونية» بهدف إرغام المواقع الشبكية على عدم تتبّع مستخدمي الإنترنت».
Ars Technica,
<http://arstechnica.com/information-technology/2014/05/eff-privacy-badger-plugin-aimed-at-forcing-websites-to-stop-tracking-users>
5. «مؤسسة الحدود الإلكترونية» (2014). تقرير: «دليل إرشادي على الإنترنت من «مركز معلومات الخصوصية الإلكترونية» بخصوص الأدوات العملية في حماية الخصوصية».
<http://epic.org/privacy/tools.html>.
6. سارة م. واتسون (16 سبتمبر 2014). قناة «الجزيرة» وموقعها الإلكتروني. مقال: «أسأل جهاز فك تشفير قنوات التلفزيون: التبرص بالضربات».
Al Jazeera,
<http://america.aljazeera.com/articles/2014/9/16/the-decoder-stalkedbysocks.html>
7. شركة «مايكروسوفت» (21 أغسطس 2013). تقرير: «نظرة عامة على برنامج «بيت لوكر»».
<http://technet.microsoft.com/en-us/library/hh831713.aspx>.
8. شركة «آبل» (أغسطس 2012). تقرير: «أفضل السبل في توظيف «فايل فولت 2.0»».
http://training.apple.com/pdf/WP_FileVault2.pdf.
9. جيمس لين (29 مايو 2014). مجلة فوربس. مقال: «برنامج التشفير «تروكريب» يختفي في سحابة من الأسرار».
Forbes

<http://www.forbes.com/sites/jameslyne/2014/05/29/open-source-crypto-truecrypt-disappears-with-suspicious-cloud-of-mystery>.

10. نيكيتا بوديسوف وإيان غولديبرغ وإريك بريوار (28 أكتوبر 2004). منتدى في واشنطن عن «الخصوصية في المجتمع الإلكتروني». ورقة بحث: «محادثات غير قابلة للتسجيل، أو، لماذا لا تستعمل برنامج «خصوصية معقولة جدًا» (Pretty Good Privacy) [اختصاراً «بي جي بي» PGP]؟».
11. ستيفان سوموغي (3 يونيو 2014). مدونة إلكترونية «غوغل سيكيورتي أون لاين». تقرير: «تسهيل عملية تشفير التواصل بين نقطتي الإرسال والتلقي».

Google Online Security Blog,

<http://googleonlinesecurity.blogspot.com/2014/06/making-end-to-end-encryption-easier-to.html>

12. تيم ديركز وإريك رسكورلا (17 أبريل 2014). موقع «قوة المهمة بشأن هندسة الإنترنت». تقرير: «النسخة 1.3 من «ترانسبورت لاير سيكيوريتي»».

<http://tools.ietf.org/html/draft-ietf-tlsrfc5246-bis-00>.

13. «مؤسسة الحدود الإلكترونية» (2014). تقرير: «إتش تي بي إس إفري وير».

<https://www.eff.org/Https-everywhere>

14. ثمة دليل إرشادي جيد. «مركز معلومات الخصوصية الإلكترونية» (2014). دليل إرشادي على الإنترنت من «مركز معلومات الخصوصية الإلكترونية» بخصوص الأدوات العملية في حماية الخصوصية.

<http://epic.org/privacy/tools.html>.

15. بيتر برايت ودان غوبن (14 يونيو 2013). موقع «أرس تكنيكا». مقال: «بريد إلكتروني مشفر: كم من العناء تحتل لقاء إبعاد «وكالة الأمن القومي» عنك؟».

Ars Technica,

<http://arstechnica.com/security/2013/06/encrypted-e-mail-how-much-annoyance-will-you-tolerate-to-keep-the-nsa-away>.

16. يتضمن النص التالي رأي «قوة المهمة لهندسة الإنترنت» عن الخصوصية والتضد الواسع. مدونة إلكترونية لدعوة المهمة لهندسة الإنترنت. جاري أركو وستيفان فاريل (7 سبتمبر 2014). تقرير: «الخصوصية والتضد الواسع».

«Security and pervasive monitoring», Internet Engineering Task Force,

<https://www.ietf.org/blog/2013/09/security-and-pervasive-monitoring>

17. أندى غرينبرغ (21 مايو 2014). مجلة وايرد. مقال: «تطبيق مجاني يتيح لسنودن المستقبل إرسال ملفات ضخمة بأمان مع إغفال الهوية».

Wired,

<http://www.wired.com/2014/05/onionshare>.

18. ميريمير [مجلة عن برنامج عزل الخوادم يستخدمه الهاكرز] (2014). مقال: «خصوصية متطورة وإغفال الهوية باستخدام برامج «في أم أس» و«في بي أن» و«تور» وغيرها».

IVPN,

<https://www.ivpn.net/privacy-guides/advanced-privacy-and-anonymity-part-1>.

19. معظم التلاجات الحديثة لا تتمتع بهياكل معدنية صلبة، ولا تصلح لمهمة عزل الموجات الكهرومغناطيسية الصادرة عن الخلوي. دق في موديل ثلاثتك قبل أن تستخدمها لذلك الغرض.
20. جون فاربيه (16 أبريل 2014). موقع «نياتوراما». مقال: «ما هي الوظيفة التي لا توجد إلا في بلدك؟».

Neatorama,

<http://www.neatorama.com/2014/04/16/What-Is-a-Job-That-Exists-Only-in-Your-Country>

21. روبنسون ماير (24 يوليو 2014). مجلة أتلانتيك. مقال: «تمويه وجهك ليكون مضاداً للرقابة».

Atlantic,

<http://www.theatlantic.com/features/archive/2014/07/makeup/374929>.

جوزيف كوكس (14 سبتمبر 2014). موقع «كيرنل». مقال: «صعود الحركة المضادة لتقنيات التعرف إلى الوجه».

Kernel,

<http://kernelmag.dailydot.com/issue-sections/features-issue-sections/10247/anti-facial-recognition-movement>.

22. آدم هارفي (2013). «أردية شبكية».

<http://ahprojects.com/projects/stealth-wear>

23. يحتوي المقال التالي قائمة عن تلك التقنيات. فن برنتون وهيلين نيسمباوم (2 مايو 2011). صحيفة فرست مونداي الإلكترونية. مقال: «مقاومة عامة لجمع البيانات وتحليلها: نحو نظرية سياسية لتعمية المعلومات». *First Monday* 15,

<http://firstmonday.org/article/view/3493/2955>.

24. تظهر الخدعة عينها في رواية روبرت أ. هاينلاين نجمة مزدوجة (1956). دار «دويل داي». <http://books.google.com/books?id=bnoGAQAIAAJ>.

25. دانا بويد (7 نوفمبر 2011). صحيفة فرست مونداي الإلكترونية. مقال: «لماذا يشجع الآباء أطفالهم على مخادعة «فيسبوك» بشأن العمر: آثار غير مقصودة مقصود لدقانون حماية خصوصية الأطفال». *First Monday* 16,

<http://firstmonday.org/ojs/index.php/fm/article/view/3850/3075>.

26. من المهم التغلب على ذلك الاستهجان. هناك قصة عن مستخدم رفض أن يعطي موقع «كومكاست» سبباً لخروجه من خدمة ذلك الموقع. في البداية، يبدو الأمر فظاً. لكن، إذا أمعنت التفكير في الأمر، يتبين لك أن «كومكاست» ليس مخوّل الحصول على تلك المعلومة. زيني جاردن (14 يوليو 2014). موقع «بوينغ بوينغ». مقال: «أصغ إلى «كومكاست» مضطهداً لريان بلوك وفيرونيكا بلمونت، أثناء محاولتهما إلغاء الخدمة».

Boing Boing,

<http://boingboing.net/2014/07/14/listen-to-comcast-torture-ryan.html>.

27. وضعت جوليا أنغوين كتاباً ممتازاً عن تجربتها في التملص من الرقابة في عصر الإنترنت. جوليا أنغوين (2014). دار «تايمس بوك». كتاب: الأمة في شبكة الصيد: الرغبة في الخصوصية، الأمن والحرية في عالم الرقابة التي لا تكل.

Times Books,

<http://books.google.com/books?id=bbS6AQAQAQBAJ>.

28. آثار ستيوارت باركر هذه النقطة. ستيوارت أ. باركر (29 أكتوبر 2013). شهادة أمام اللجنة المنتقاة الدائمة بشأن الاستخبارات الأميركية في مجلس النواب. «إصلاحات ممكنة لقانون الاستخبارات الأجنبية».

Representatives,

<http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Baker10292013.pdf>

29. ديفيد سانغر (13 أغسطس 2013). صحيفة نيويورك تايمس. مقال: «التسريبات بشأن وكالة الأمن القومي»، تخفض إمكان وضع خطة للدفاع السبراني».

New York Times,

<http://www.nytimes.com/2013/08/13/us/nsa-leaks-make-plan-for-cyberdefense-unlikely.html>

30. دي. آل. إيه باير (7 مارس 2013). دراسة «قوانين حماية البيانات في العالم».

http://files.dlapipe.com/files/Uploads/Documents/Data_Protection_Laws_of_the_World_2013.pdf

31. في العام 2014، جُزيت «مايكروسوفت» تحدي طلب أميركي حكومي بشأن بيانات الشركة مخزنة حصرياً في إيرلندا. وطلبت المحكمة من «مايكروسوفت» تسليم بياناتها إلى الحكومة الأميركية. وما زال القرار معلّقاً بانتظار حكم الاستئناف. جوزيف أكس (31 يوليو 2014) وكالة «رويترز» للأنباء. مقال: «محكمة أميركية تطلب من «مايكروسوفت» تسليم رسائل بريد إلكتروني لمستخدمين، آتية من الخارج».

Reuters,

<http://www.reuters.com/article/2014/07/31/usa-techwarrants-idUSL2N0Q61WN20140731>

32. صحيفة الغارديان (19 سبتمبر 2014). مقال: «منح سفير بريطاني سابق في الولايات المتحدة، نفاذاً إلى البيانات».

Guardian,

<http://www.theguardian.com/technology/2014/sep/19/sir-nigel-shienwald-data-access-role-david-cameron>

33. ريتش موغول (25 يونيو 2014). مجلة ماك وورلد. مقال: «لماذا تهتم «آبل» فعلياً بخصوصيتك؟»

Macworld,

<http://www.macworld.com/article/2366921/why-apple-really-cares-about-your-privacy.html>

تشارلز آرثر (18 سبتمبر 2014). صحيفة الغارديان. مقال: «تيم كوك، رئيس «آبل»، يهاجم «غوغل» و«فيسبوك» بسبب ثغرات في الخصوصية».

Guardian,

<http://www.theguardian.com/technology/2014/sep/18/apple-tim-cook-google-facebook-privacy-surveillance>.

34. تتيح البلدان الأوروبية لحكوماتها نفاذاً أوسع كثيراً إلى البيانات، بالمقارنة مع الولايات المتحدة. سايريس فاريفار (13 أكتوبر 2013). موقع «أرس تكنيكا». مقال: «أوروبا لن تنتفذك: لماذا ربما يكون بريدك الإلكتروني أكثر أماناً في الولايات المتحدة».

Ars Technica,

<http://arstechnica.com/tech-policy/2013/10/europe-wont-save-you-why-e-mail-is-probably-safer-in-the-us>

35. جيمس كانتر (8 أبريل 2014). صحيفة نيويورك تايمس. مقال: «حمائية للخصوصية، المحكمة الأوروبية ترفض قوانين تخزين البيانات».

New York Times,

<http://www.nytimes.com/2014/04/09/business/international/european-court-rejects-data-retention-rules-citing-privacy.html>.

36. ديفيد ماير (17 يوليو 2014). مقال: «صار القانون «الطارئ» البريطاني «درب» للرقابة أمراً واقعاً الآن».

<http://gigaom.com/2014/07/17/the-uks-emergency-drip-surveillance-law-is-now-a-done-deal>

37. راي كوريفان (11 يوليو 2014). مقال: «الرقابة العامة والساسة المزعورون».

<http://b2fxxx.blogspot.com/2014/07/masssurveillance-and-scared-politicians.html>.

38. من بيننا مواقع «نو سي سي تي في»

http://www.no-cctv.org.uk/camera_locations/default.asp

و«سي سي تي في» في تراجر هانت»

<http://cctvtreasurehunt.wordpress.com>.

و«إن واي سي سيرفالنس كاميرا بروجكت»

<http://www.mediaeater.com/cameras>.

39. كريستيان (24 يونيو 2004). موقع «جنوب» الإلكتروني. مقال: «عقب تظاهرات ضخمة السبت ضد قانون «إن إي آي إس» (NEIS)، حكومة كوريا الجنوبية تبرهن على تفهمها للديمقراطية».

Jinbo,

<http://act.jinbo.net/drupal/node/5819>.

سيونغ كيم وسونهو كيم (أكتوبر 2004). مقال: «الصراع على استخدام تقنيات المعلوماتية في المدارس الكورية».

<http://ajou.ac.kr/~seoyong/paper/Seoyong%20Kim-2004-The%20Conflict%20Over%20the%20Use%20of%20Information%20Technology.pdf>.

40. شركة «آي بي أم» (16 كانون أول 2004). تقرير: «مخزن «فيوتشر ستور» التابع لمجموعة «مترو»، يصدم الجمهور العام في ألمانيا- بفضل التكنولوجيا اللاسلكية».

ftp://ftp.software.ibm.com/software/solutions/pdfs/10704035_Metro_cs_1b.pdf.

كيم زيتّر (28 فبراير 2004). مجلة وايرد. مقال: «الألمان يحتجّون على خطط لصنع هويّات بالموجات اللاسلكيّة لهم».

Wired,

<http://archive.wired.com/techbiz/media/news/2004/02/62472>.

41. ك. س. جونز (17 فبراير 2009). مجلة إنفورمايشن ويك. مقال: «شروط جديدة من «فيسبوك» تثير احتجاجاً».

Information Week,

<http://www.informationweek.com/software/social/facebook-terms-of-use-draw-protest/d-id/1076697>.

بوبي جونسون وآفوا هيرش (18 فبراير 2009). صحيفة الغارديان. مقال: «فيسبوك» يتراجع عقب احتجاجات شبكيّة».

Guardian,

<http://www.theguardian.com/technology/2009/feb/19/facebook-personal-data>

42. أشلي هالساى الثالث ودريك كرافتز (25 نوفمبر 2010). صحيفة واشنطن بوست. مقال: «احتجاجات على التفتيش اليدوي من قبل «أمن إدارة النقل»، وماسحات الجسد لا تؤخّر رحلات «عيد الشكر»».

Washington Post,

<http://www.washingtonpost.com/wp-dyn/content/article/2010/11/24/AR2010112406989.html>

43. إنّها فكرة التغيير التراكمي، أو الدفع بالتشويش. شارلز ي. ليندبلوم (ربيع 1959). مجلة بابليك أدمنسترايشن ريفيو. مقال: «علم «الدفع بالتشويش»».

الفصل 16: الأعراف الاجتماعية ومقايضة «البيانات الضخمة»

1. بول بلومنتال (2 مارس 2009). «مؤسسة صن لايت». تقرير: «لا يملك الكونغرس وقتاً لقراءة «قانون باتريوت» الأمريكي».

Sunlight Foundation,

<http://sunlightfoundation.com/blog/2009/03/02/congress-had-no-time-to-read-the-usa-patriot-act>.

2. ليونيل هاددي وستانلي فيلدمان (سبتمبر 2011). مجلة أميركان سايكولوجست. مقال: «الأميركيون يردّون سياسياً على 11/9: فهم تأثير ضربات الإرهاب وعقابيلها».

American Psychologist 66,

<http://www.ncbi.nlm.nih.gov/pubmed/21823777>.

3. تيم داوسون (9 يونيو 2014). «الاتحاد القومي للصحافيين [الأميركيين]». مقال: «أقرب إلى «الستازي» منه إلى جيمس بوند».

National Union of Journalists,

<http://www.nuj.org.uk/news/more-like-the-stasi-than-james-bond>.

4. جوزيف كامبوس الثالث (7 سبتمبر 2013). جامعة أوكسفورد. «الذاكرة والتذكّر: انتشار الخوف والرعب والإرهاب، في التحكّم والشرعية».

<http://www.inter-disciplinary.net/at-the-interface/wp-content/uploads/2013/07/camposfhtpaper.pdf>

5. جاك غولد سميث (9 أغسطس 2013). مدوّنة الكترونيّة «لوفير». مقال: «تأملات عن الإفراط على «وكالة الأمن القومي» مع توقع أنّ سلطات «وكالة الأمن القومي» (والإشراف والشفافية) سوف تتوسع».

Lawfare,

<http://www.lawfareblog.com/2013/08/reflections-on-nsaoversight-and-a-prediction-that-nsa-authorities-and-oversight-and-transparencywill-expand>.

6. دوناج. بير-موني (أغسطس 2009). «جامعة هاواي» في «مانوا». كتاب: عن الإرهابيين والطفافة والاضطراب الاجتماعي: نموذج نظري عن تنافس المخاوف لتطوير قانون يتصل بالخصوصية في الاتصالات بمواجهة رقابة قوى إنفاذ القانون الأميركية.

University of Hawai'i at Manoa,

<http://books.google.com/books?id=8LveYgEACAAJ>

- كيفن ج. روبي (2012). مطبعة جامعة شيكاغو. كتاب: المجتمع والدولة والخوف: إدارة الأمن القومي والحدود بين الذعر والرؤى عن الذات.

University of Chicago Press,

<http://books.google.com/books?id=UPILnwEACAAJ>.

7. داون روث وستيفن موزاتي (نوفمبر 2004). مقال: «الأعداء في كل مكان: الإرهاب والذعر الأخلاقي والمجتمع المدني الأمريكي».

http://www.researchgate.net/publication/227209259_Enemies_Everywhere_Terrorism_Moral_Panic_and_US_Civil_Society/file/32bfe50d3c7fe0d03b.pdf

- ديفيد روثكوف (6 أغسطس 2013). مجلة فورين آفيرز. مقال: «أخطار حقيقية».

Foreign Policy,

http://www.foreignpolicy.com/articles/2013/08/06/the_real_risks_war_on_terror

8. إنه الأمن على مدار السنة. بروس شنابر (22 فبراير 2007). مجلة وايرد. مقال: «لماذا يأتي رجال الشرطة الأذكاء أموراً غريبة؟».

Wired,

<http://archive.wired.com/politics/security/commentary/securitymatters/2007/02/72774>.

9. في الوثائق المسربة من «وكالة الأمن القومي»، هناك أقوال تشير تحديداً إلى 11/9: «أنا أفضل أن أكون هنا اليوم لأشرح هذه البرامج، على أن أشرح حادثاً آخر يشابه 11/9 لم تكن قادرين على منعه». جاسون ليوبولد (30 أكتوبر 2013). قناة «الجزيرة» التلفزيونية. مقال: «كُشف أخيراً: استخدمت «وكالة الأمن القومي» حادث 11/9 كمفتاح صوتي في تبرير رقابتها».

Al Jazeera,

<http://america.aljazeera.com/articles/2013/10/30/revealed-nsa-pushed911askeysoundbitetotjustifysurveillance.html>.

10. كلاي شيركي (14 مارس 2010). ملاحظات في برنامج تلفزيوني في «أوسطن» بولاية تكساس، اقتبسها كيفن كيللي (2 أبريل 2010) في مقال: «مبدأ شيركي».

Kevin Kelly,

<http://kk.org/thetechnium/2010/04/the-shirky-prin>.

11. جاك غولد سميث (9 أغسطس 2013). مدونة الكترونية «لوفير». مقال: «تأملات عن الإشراف على «وكالة الأمن القومي» مع توقع أن سلطات «وكالة الأمن القومي» (والإشراف والشفافية) سوف تتوسع».

Lawfare,

<http://www.lawfareblog.com/2013/08/reflections-on-nsaoversight-and-a-prediction-that-nsa-authorities-and-oversight-and-transparencywill-expand>.

12. أعتقد شخصياً بأن الناس في كوريا وكوريا الشمالية في مأمن من الإرهاب، ولكن بأي ثمن؟
13. بروس شنابر (17 مايو 2007). مجلة وايرد. مقال: «دروس من الهجوم في «جامعة فرجينيا»: المخاطر النادرة تولد ردود أفعال لا عقلانية».

Wired,

http://archive.wired.com/politics/security/commentary/securitymatters/2007/05/securitymatters_0517

14. ترجع العبارة إلى أوقات قديمة، وجاءت ضمن قرار من «المحكمة العليا»: «ليس أننا نختار بين الحرية والنظام،

بل نختار بين الحرية مع النظام من جهة، والفوضى من كليهما من الجهة الثانية. هناك خطر من عدم قيام المحكمة بمزج منطقها القانوني مع شيء من الحكمة الآتية من الممارسة، في تحويل «وثيقة حقوق المواطن» الدستورية إلى حلف انتحاري». قرار من «المحكمة العليا» (16 مايو 1949).

<http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=us&vol=337&invol=1>.

15. يوجد كتاب استقى عنوانه من تلك العبارة. ريتشارد أ. بوسنر (2006). مطبعة جامعة أوكسفورد. كتاب: ليس حلفاً انتحارياً: الدستور في زمن الطوارئ القومية.

Oxford University Press,

<http://books.google.com/books?id=hP6PAAAAAMAAJ>.

16. ريتشارد أورانج (14 أبريل 2012). صحيفة الغارديان. مقال: «الرد على الكراهية بالحب: كيف حاولت النرويج التغلب على الذعر الذي سببه أندرياس بريفيك».

Guardian,

<http://www.theguardian.com/world/2012/apr/15/anders-breivik-norway-copes-horror>

تيم كوشينغ (26 يوليو 2012). موقع «تيك درت». مقال: «بعد سنة من مجزرة بريفيك، تتابع النرويج مكافحة الإرهاب بالديمقراطية والانفتاح والحب».

Tech Dirt,

<https://www.techdirt.com/articles/20120724/20363519819/one-year-after-breivik-massacre-norway-continues-to-fight-terrorism-with-democracy-openness-love.shtml>

17. بروس شنابر (7 يناير 2012). موقع «إيه أو آل نيوز». مقال: «رد فعلنا هو الفشل الحقيقي للأمن».

AOL News,

https://www.schneider.com/essays/archives/2010/01/our_reaction_is_the.html

18. جون مولر ومارك ستيوارت (2011). «مطبعة جامعة أوكسفورد». كتاب: إرهاب، أمن ونقود: التوازن بين المخاطر والفوائد والتكاليف في وزارة الأمن الوطني.

Oxford University Press, chap. 2,

<http://books.google.com/books?id=jyYGL2jZBC4C>

19. حتى إنني ألقت كتاباً بهذا العنوان. بروس شنابر (2003). دار «ويلي» للنشر. كتاب: ما وراء التفكير بتعقل عن الأمن في عالم يغيب غير مستقر.

Wiley,

<http://books.google.com/books/about/?id=wuNImmQufGsC>.

20. تحتاج أستاذة القانون في «جامعة نيويورك» هيلين نسينباوم، بأن الخصوصية لا تفهم إلا ضمن السياق والتوقعات. هيلين نسينباوم (خريف 2011). دراسة: «مقاربة سياقية للخصوصية على الإنترنت».

http://www.amacad.org/publications/daedalus/11_fall_nissenbaum.pdf

أليكس مادريغال (29 مارس 2012). مجلة «آتلانتيك». مقال: «الفيلسوف الذي ترك بصماته على السياسة الجديدة لـلجنة التجارة الفيدرالية، بشأن الخصوصية».

Atlantic,

<http://www.theatlantic.com/technology/print/2012/03/the-philosopher-whose-fingerprints-are-all-over-the-fts-new-approach-to-privacy/254365>.

21. يعني ذلك أن الفروقات الإقليمية ستستمر في الإنترنت، على الرغم من أن طبيعتها العالمية تقتضي انسجاماً أكثر.

22. سارة غريدار كرونان ونيل ف. بايلين (5 أبريل 2007). «رابطة المحامين الأميركيين». مقال: «هل يجدر بي البحث عن أعضاء هيئة المحلفين على «غوغل»؟ واعتبارات أخلاقية أخرى».

American Bar Association,

http://apps.americanbar.org/litigation/committees/products/articles/0407_cronan.html

23. سامانثا هنغ (مارس 2013). موقع «غلامور». مقال: «لم يجدر بك التوقع عن المواعدة عبر «غوغل»؟»

Glamour,

<http://www.glamour.com/sex-love-life/2013/03/why-you-should-stop-googling-your-dates>.

هناك شريط فيديو يظهر المدى المريب الذي بلغته تلك الأشياء. ماريو كونتريراس (29 مايو 2014). «اللقاء في مكان عام».

<http://vimeo.com/96870066>.

24. اندريا بارتز وبرينا إيهريش (7 ديسمبر 2011). شبكة «سي أن أن». مقال: «ما يجب وما لا يجب في البحث عن الناس على «غوغل»».

CNN,

<http://www.cnn.com/2011/12/07/tech/social-media/netiquette-google-stalking>.

25. جوي كوسكاريلي (12 ديسمبر 2010). مقال: «هل يملك جوليان أسانج بروفایل على «أوكي كيوبيد»؟» http://blogs.villagevoice.com/runninscared/2010/12/does_julian_ass.php.

26. مجلة الإيكونوميست (5 يونيو 2014). مقال: «تجّار البؤس».

Economist,

<http://www.economist.com/news/international/21606307-howshould-online-publication-explicit-images-without-their-subjects-consent-be>.

27. ديفيد كرافتس (15 يوليو 2013). مجلة وايرد. مقال: «مواقع إزالة «صور الاعتقال» مدانة بالابتزاز».

Wired,

<http://www.wired.com/2013/07/mugshot-removal-extortion>.

ديفيد سيغال (6 أكتوبر 2013). صحيفة نيويورك تايمس. مقال: «معتقل بصور الاعتقال على الإنترنت».

New York Times,

<http://www.nytimes.com/2013/10/06/business/mugged-by-a-mug-shot-online.html>.

28. ديفيد برين (1998). دار: «بلازك بوكس». كتاب: المجتمع الشفاف: هل ترغما التكنولوجيا على الاختيار بين الخصوصية والحرية؟

<http://www.davidbrin.com/transparentociety1.html>

29. إميلي نوسباوم (12 فبراير 2007). مجلة نيويورك ماغازين. مقال: «قل كل شي».

New York Magazine,

<http://nymag.com/news/features/27341>.

30. جيسي إروين (7 أكتوبر 2014). موقع «موديل فيو كالتشر». مقال: «تهئية الطلاب لرقابة مدى العمر».

Model View Culture,

<http://modelviewculture.com/pieces/grooming-students-for-a-lifetime-of-surveillance>

31. تطلب بعض المدارس من الطلبة ارتداء شارات إلكترونية، وهي التقنية عينها التي يستخدمها المزارعون مع قطعان الماشية. وكالة أنباء «أستوشيتدبرس» (11 أكتوبر 2010). مقال: «مدارس في منطقة «هوستون» تتبع التلامذة بشارات تعمل بالإشارات اللاسلكية».

<http://www.dallasnews.com/news/education/headlines/20101011-Houston-area-schools-tracking-students-with-6953.ece>

32. الأمم المتحدة (10 ديسمبر 1948). وثيقة: «الإعلان العالمي لحقوق الإنسان».

<http://www.un.org/en/documents/udhr>

33. جرت مراجعة الميثاق في 2010. «الحكمة الأوروبية لحقوق الإنسان» (1 يونيو 2010). «الميثاق الأوروبي لحقوق الإنسان»، «المجلس الأوروبي».

http://www.echr.coe.int/documents/convention_eng.pdf

34. دوغ ليندر (2014). جامعة ميسوري. بحث: «تقيص التضاربات الدستورية: الحق في الخصوصية».

<http://law2.umkc.edu/faculty/projects/ftrials/conlaw/rightofprivacy.html>.

35. الاتحاد الأوروبي (18 ديسمبر 2000). «إعلان الحقوق الأساسية في الاتحاد الأوروبي».

- http://ec.europa.eu/justice/fundamentalrights/charter/index_en.htm.
36. تعيد الوثيقة التأكيد على «الحق الإنساني في الخصوصية، وبموجبها لا يتعرض فرد لتدخل اعتباطي أو غير شرعي في خصوصيته أو خصوصيتها، وكذلك الحال بالنسبة للمنزل والعائلة والمراسلات. ويملك أيضاً الحق في الحماية قانونياً ضد ذلك التدخل. وتقر [الأمم المتحدة] أنَّ ممارسة الحق في الخصوصية مهم بالنسبة لتحقيق الحق في حرية التعبير، وحرية تبني الأفكار من دون تدخل، وهو [الحق في الخصوصية] من أسس المجتمع الديمقراطي». الجمعية العامة للأمم المتحدة (21 يناير 2014)، قرار تبنته الجمعية العامة، في 18 ديسمبر 2013، 167/68، «الحق في الخصوصية في العصر الرقمي».
- http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/68/167.
37. أُعلِّنت الشريعة في العام 2000، لكنها لم تكتسب قوة القانون إلا بعد إقرارها جزءاً من «اتفاقية لشبونة» في 2009. الاتحاد الأوروبي (18 ديسمبر 2000). «شريعة الحقوق الأساسية في الاتحاد الأوروبي».
- http://ec.europa.eu/justice/fundamental-rights/charter/index_en.htm.
38. قال الرئيس الأميركي بنجامين فرانكلين: «أولئك الذين يتخلّون عن حرية أساسية ليشتروا القليل من الأمن المؤقت؛ لا يستحقون الحرية ولا الأمن».
39. مارسيا ستينبانك (8 أغسطس 2013). جامعة ستانفورد. مقال: «تأثير سنودن: فرصة؟»
- http://www.ssiereview.org/blog/entry/the_snowden_effect_an_opportunity.
40. جيرالد ف. سايب (21 نوفمبر 2008). صحيفة وول ستريت جورنال. مقال: «في الأزمة، هناك فرصة لأوباما». *Wall Street Journal*, <http://online.wsj.com/news/articles/SB122721278056345271>.
41. بروس شنابير (2012). كتاب: كَذِبَة ومتمردون: تفعيل الثقة التي يحتاجها المجتمع لينمو. دار «ويلي» للنشر.
- <http://www.wiley.com/WileyCDA/WileyTitle/productCd-1118143302.html>.
42. شارلز سافران وآخرون (يناير/فبراير 2007). مجلة رابطة المعلوماتية الطبية الأميركية. بحث: «نحو إطار قومي للاستخدام الثانوي للبيانات الصحية: ورقة بيضاء من «رابطة المعلوماتية الطبية الأميركية»». *Journal of the American Medical Informatics Association* 14, <https://www.sciencedirect.com/science/article/pii/S106750270600212X>.
- بيتر جانسن ولارس جانسن وتسورن برونك (يونيو 2012). مجلة نايتشر. بحث: «التقيب في السجلات الصحية: نحو تحسين التطبيقات البحثية والرعاية الطبية».
- Nature Reviews: Genetics* 13, http://www.dartmouth.edu/~cbbc/courses/bio270/PDFs-13S/Tim_Byounggug.pdf.
43. راينول جونكو (2014). بحث: «انخراط الطلبة عبر الدسوشال ميديا: ممارسات مبنية على الأدلة كي تستخدم في العلاقات مع الطلاب».
- <http://www.wiley.com/WileyCDA/WileyTitle/productCd-1118647459.html>.
44. كريستيان رودر (28 يوليو 2014). موقع «أو كيه تريند». مقال: «نحن نجري تجارب على البشر!»
- OK Trends*, <http://blog.okcupid.com/index.php/we-experiment-on-human-beings>
- كريستيان رودر (4 سبتمبر 2014). صحيفة وول ستريت جورنال. مقال: «عندما تسترق المواقع الشبكية النظر إلى الحياة الخاصة».
- Wall Street Journal*, <http://online.wsj.com/articles/when-websitespeek-into-private-lives-1409851575>.
45. مارك فاينشتاين (4 سبتمبر 2014). صحيفة هافنغتون بوست. مقال: «أو كي كيوييد» بالآخرى أنه «أو كي» غبي».
- Huffington Post*, http://www.huffingtonpost.com/mark-weinstein/okcupid-thats-okstupid_b_5739812.html.
46. المكتب التنفيذي للرئيس أوباما (2013). وثيقة: «الحكومة الإلكترونية: بناء منصة القرن 21 كي تخدم الشعب الأميركي بصورة أفضل».

<http://www.whitehouse.gov/sites/default/files/omb/egov/digital-government/digital-government.html>.

شركة «مايكروسوفت» (27 مارس 2013). مركز أنباء «مايكروسوفت». تقرير: «تبني الدولة والحكومات المحلية تقنية «سي آر أم» داينامكس من مايكروسوفت، بهدف الارتقاء بمستوى تقديم الخدمات للمواطن».

Microsoft News Center,

<http://www.microsoft.com/en-us/news/press/2013/mar13/03-27dynamicscrmp.aspx>.

47. تبدي «القيادة الحكومية للاتصالات» في بريطانيا، خشيتها علناً من ذلك النقاش. إذ تحدثت إحدى وثائق سنودن عن محادثات لتجنيب «النقاش العام المؤذي» عن مدى الرقابة. جيمس بول (25 أكتوبر 2013). صحيفة الغارديان. مقال: «الكشف عن مذكرات سرية تبين جهود «القيادة الحكومية للاتصالات» للإبقاء على الرقابة العامة سرًا».

Guardian,

<http://www.theguardian.com/uk-news/2013/oct/25/leaked-memos-gchq-mass-surveillance-secretsnowden>.

48. عملياً، تلك العبارة هي اقتباس لمارتن لوثر كينغ من نص لثيودور باركر، وكان من دعاة إزالة الفوارق العنصرية، في العام 1835، يرد فيه: «لا أظاهر بأنني أفهم الكون الأخلاقي؛ لأن قوسه ضخم، فيما لا تتصل عيناى لسوى الطرق الصغيرة. لا أستطيع احتساب القوس بأكمله ومتابعته بتجربة البصر؛ لكنني أستطيع تخمينه ضميراً. ولكن، استناداً إلى ما أراه، أنا متأكد أنه يتجه صوب العدالة». غارسون (15 نوفمبر 2012). قاموس تقصي الاقتباسات. «كون الأخلاق له قوس طويل لكنه يتجه صوب العدالة».

Quote Investigator,

<http://quoteinvestigator.com/2012/11/15/arc-of-universe>.

الفهرس

386، 411-413، 415، 451، 460،

465-466، 468، 484-485، 502

الاختلالات المنهجية 163-164، 249

أدبوك بلاس 96

أدوردرز 94

إدارة المخاطر 218

إدارة علاقات المستهلك («سي آر أم») 90،

510

إدارة مكافحة المخدرات 112، 165،

441

أدوات طبية متصلة بالإنترنت 32، 366

أدوب 85، 102

آر إس إيه (شركة أمن) 121، 412

آرامكو 126، 416

آرنباك، أكسل 269، 484

إرهاب، حريات مدنية 16، 153، 209،

338-339، 405، 484؛ قواعد بيانات

حكومية 115، 153، 404؛ كتيب للرقابة

العامة 16-17، 107، 117، 164، 215،

274؛ الرقابة العامة بوصفها أداة غير فعالة

لكشف 116، 147، 210-211، 215،

462-464؛ إرهايو الـ «إيغور» 326،

418

بروتوكول 320، 382

- 1 -

أبل 56، 88، 98، 100-102، 129،

191، 199، 204، 232، 275، 309،

320، 328، 366، 377، 391، 398،

452، 455، 471، 486، 497، 498،

499، 501، 504

أبواب خلفية (فيروسات حاسوبية) 187،

227، 255، 274، 486

الاتحاد الأوروبي 127، 130، 132، 254،

276، 286، 292، 299، 312، 329،

343، 351، 415، 417، 421، 440،

480، 492، 495، 500، 508، شرعة

الحقوق الأساسية 344، 509، توجيه بشأن

حماية المعلومات 243، 490، 493؛ قوانين

الاحتفاظ بالبيانات 420

الاتحاد الدولي للاتصالات 281

اتفاقيات عدم الكشف 114

إثيوبيا 123

أجهزة إلكترونية، سيطرة الشركة البائعة 61

الأخ الصغير (رواية) 85، 323

اختراق ديجينوتار 119، 410

اختراق، هكرز 14، 20، 74-75، 120،

122، 181، 183-184، 202، 219،

220، 222، 229، 231، 273،

البيانات 18؛ تنقيب في المعلومات 59،
211؛ تناقص قيمة 95-97، 395، 396؛
في «جي مايل» 43، 67، 220، 459؛ رقابة
الإنترنت 180؛ البيانات المكانية 43، 55،
385؛ ادعاءات مبالغ فيها 348، 394؛
في الحملات السياسية 59، 93، 180،
393، 450؛ الرقابة الشاملة 43، 55،
92، 344، 449؛ إعلان حقوق الإنسان
والمواطن 313، 343، 508؛ إعلان مدريد
للخصوصية 314-315، 501؛ إعلان
موجه 61، 87، 89، 362، 393، 394،
450
إغفال الهوية 206-207، 314، 317،
322، 346، 387، 444، 457، 461،
502
أفغانستان 48، 109، 326، 424
الأكاديميات الوطنية 486
أكراد 127، 417
أكريث هيلث (مؤسسة) 169، 443
إكزاكت داتا 73
أكزيكوم 91، 378، 386
إكس كي سكور 64، 371، 381
إلبايت سيستمز 134، 423
إلسبرغ، دانيال 159، 437، 438
إلكومسوفت 232
ألمانيا 274، 372، 455، 504، ألمانيا
الشرقية 44، 372؛ التحكم في الإنترنت
127، 150، 389، 489، 491، رقابة
«وكالة الأمن القومي» 127، 191، 233،
245، 264، 407، 427، 454، رقابة
على المواطنين 116، 142، 282، 433،

أسانج، جوليان 341، 508
استخدام «البيانات المكانية» 12، 15،
69، 78، 105، 131، 362، 364، 384،
388، 481
أستراليا، الشراكة الدولية في الاستخبارات
124
استقلالية 474
إستونيا، هجمات سبرانية 152، 205،
416، 460
إسرائيل 141-142، 250، 274، 326،
486؛ التعرف إلى فريق اغتيال 75، 386
أسلحة الدمار الشامل 147
اشتراكية 174، 340
إشراف تكتيكي 247-248، 267؛
إشراف على رقابة الشركات انظر أيضاً رقابة
عامة حكومية 120، 158، 246، 259،
260-261، 263، 266، 277؛ إشراف
وموثوقية 246، 294
أشرطة انتقام (الجنس الإباحي) 164، 440
إطار الخصوصية 286-287، 294، 490؛
«منظمة التنمية والتعاون الاقتصادي»
286، 490، 493
أعراف اجتماعية 335، 342، 395، 505،
الخوف 337، 339، 347، الحرية 335،
رقابة عامة 335، 342، 349، الخصوصية
341، 343، 395، 491
الإعلان الدولي لحقوق الإنسان 343
الإعلان المُشخص 378، 447؛ من
آمازون 89، 99، 391؛ من آبل 18، 46،
328؛ عنصر الريبة في 95، 381، 394؛
سباسة المعلومات انظر صناعة سمسة

- عدوياً؛ 214؛ تكاليف 109، 122، 219،
287، 292؛ 319؛ التنقيب في المعلومات
كأداة غير فعالة 201، 210، 211، 213،
262؛ انعدام الأمان 22، 152، 232،
238، 338؛ التعمّد على الإنترنت 133،
218؛ التشفير 113، 138، 140، 141،
185-188، 217، 221-222، 228،
229، 241؛ الخوف 17، 337؛ الرقابة
العامة وضررها على الأمن 161، 225،
233، 269، 272، 275؛ التركيز خطأً
على الحوادث المشهّدية، مغالطة سردية 44،
210، 333؛ الخصوصية 64، 68، 237،
239؛ إدارة المخاطر 13، 218، 346؛
الأعراف الاجتماعية 176، 350؛ رقابة
20، 43، 45، 65، 112، 119، 129،
190، 221، 262، 326؛ ثغرات 223
أمير أحمدى، هوشانغ 163
إنترنت 19، 367، 368، 467، 97، 346؛
الإنترنت رقابة 33، 52، 73، 94؛ الإعلان
انظر الإعلان المُشخّص 83، 88، 94؛
شركات الكابل 173، 309؛ الـ"كوكيز"
83؛ شامل 173، 333؛ كلفة القدرة 121؛
شركات تقارير الشفافية 242-243،
257؛ "وكالة الأمن القومي" 15؛ إغفال
الهوية 111، 203، 206-208، 314،
317، 322، 346؛ فوائد 15-16؛ غياب
الأمكنة العامة 117، 283، 285؛ هجمات
سبرانية انظر أيضاً تسليح سبراني 327،
414-416، 460، 465، 467، 485،
488؛ تعمد انعدام الأمان 22، 238-
239، 287؛ الأزمنة الأولى 30؛ نموذج
العلاقات مع الولايات المتحدة 127-
128، 345، 417، 472
آمازون 51، 76، 98، 102، 373، 375،
398، 431؛ باعتباره وكيلاً للمعلومات
51؛ إعلان مُشخّص من 89، 99، 391
آمدوكس 274
الأمم المتحدة 508
الأمن 5-6، 9، 15، 19، 36، 39،
42، 48-50، 54، 66-67، 71،
105-108، 110-111، 116، 121،
123-125، 127-128، 139، 142،
145، 156-160، 162-165، 168،
189، 191-192، 213، 215-216،
220، 226-227، 230-231، 233،
240، 244، 246-247، 250، 253-
254، 256-261، 263-265، 267،
270-271، 273، 274، 276، 277،
279، 280-282، 288، 301، 306،
308، 309، 310، 312-313، 324،
327-332، 339، 345، 347، 354،
357، 359، 364، 369، 370-372،
374-375، 377، 379-386، 388،
390، 397، 399، 400، 402-403،
405، 407، 410-415، 417-419،
422، 426-432، 434-442، 447،
452-455، 457-464، 466-474،
476-488، 490، 492، 496-499،
501-503، 505-507، 509؛ الطائرة
241؛ هجوم مقابل دفاع 201؛ التوازن
مع الحريات المدنية 201، 209، 245،
266، 336، 340، 344، 401؛ التعقيد

آي فون 18، 46، 53، 75، 100، 101،
102، 103، 108، 275، 310، 338،
373، 377، 499
آي كلاود 88، 100، 199، 232، 471،
498
آي ماك 100، 173
إيباي (بيع إلكتروني) 97، 99، 397
إيسلون 378، 386
إيران 126؛ رقابة الحكومة، 118، 128،
135؛ هجمة سبرانية بـ«ستاكس نت»
125-126
إيريا إسبي إيه 135
آيزنهاور، دوايت 340
إيكونومست 146، 357
إيكوفاكس 92
إيمانويل رام 346
إيه أو آل 387، 447، 507
إيه تي أند تي 65، 187، 189، 204، 362،
452، 453، 497

- ب -

باركر، ثيودور 503، 510
باريزر، إيلي 179، 449
بازفيد 52
بالمر، غارات 149، 346، 460
بان أوبتيكوم 58
بانيتا، ليون 207، 373، 383، 436، 461
بايكر، ستيوارت 43، 462، 503، 507
بترايوس، ديفيد 74
بتروبراس 122
بحوث نطاظة 65-66

العمل المستند إلى الأعمال مقابل المستند
إلى الحرية 88، 93؛ حرية 19؛ الحجب
الحكومي والسيطرة 136، 149؛ تعريف
الهوية 71، 77، 203، 206؛ قوانين 246،
247؛ مصدر إعلامي 15؛ التوصيلات
الفعليّة 210؛ الخصوصية 42، 68؛ إنهاء
دور وكيل الشركة 71؛ الثقة 19، 190
أندرويد 46، 81، 100، 102، 122،
310، 388، 413، 499
إنستغرام 28، 283، 301، 373، 494
إنغل، توياس 14، 363
إنفويو إس إيه 91
أنونيموس (مجموعة «هاكرز») 75
إنشيت سيستمز 73
أوبر 14، 30، 89، 98، 172، 443، 444
أورانج 130، 365، 420، 507
أورويل، جورج، 5، 13، 85، 102،
148، 251، 334، 415، 431، 448،
457، 460
أوشوا هيغينيو (ورمر) 75
أوك ريدج، ولاية تينيسي 222
أوكرانيا 219، 326
أولبريشت روس («دريد بايريت روبرتس») 166
أونيون شير 322
آي إم إس آي كاتشرز 403
آي باد 100، 102
آي بي إم 164، 189، 371، 454، 504
آي تيونز 88، 98
آي سي ريتش 113

462، 464، 483، 490؛ تفجيرات

ماراثون 57، 115، 210، 215

بوش، جورج دبلیو (الابن) 340

بول رن (برنامیج) 140، 468

يووز، آلز هاملتون 133

بیوید، دانا 196، 268، 446، 457، 483،

503

ی آن ی باریاہ (بنک) 381

بی آن دی (الاستخبارات الألمانية) 128

بی تی 130، 412، 419

بی جی پی 320، 321، 502

بیریا، لافرینتی 146

بينغ (محرك بحث) نتائج البحوث المدفوعة

پینی پیل 441,370

بيوريا (ولاية إلينوي) 160

بیومتریक्स، بیانات 204، 458

- ٢ -

تارغت، اختراق أمني 59، 61، 95، 287،

491,465,290

تاو («عمليات الدخول المنسقة») 121،

412,281,230,140

تجسس 106، 116، 119، 120، 122،

164 163 145 128 126 123

411 400 369 244 219 168

440 432 426 420 414 412

464 463 454 453 451 442

498 497 484 472 471 470

مقابل، الرقابة 161؛ تجميع 18، 21، 39،

258, 237, 223, 215, 108, 45, 40

البرازيل، 20، 122، 124، 282

برایان، لی فان 148

بردویل، باولا 74، 386

برمودا 64، 229؛ تسجيل، «وكالة الأمن

القومي، لكل، المكالمات الهاتفية 109

320

بريد إلكتروني 411، 403، 335، 134،

455، 502، 503؛ البريد الأمريكي

خدمات برنامج «ايزوليشين كونترول اند

تم اكنف» 52؛ به يد إلك

محل، مقابل، تخزين، في سحابة رقمية 99

بسم 129، 139-140، 138

463-462,453,383

438، 499؛ جمع الـ «ميتاداتا» 34، 40،
43، 44، 64، 213، 371، 372، 381،
463، 432، 382

- ث -

ثغرات «اليوم صفر» 224، مراكمتها لدى
«وكالة الأمن القومي» 183

- ج -

جاي-زي 84
جدار النار العظيم (الدرع الذهبي) 430
جمهورية جورجيا 125، 276، 363، 491
جويون 31
جي بي إس 14، 15، 30، 34، 75، 270،
373، 484؛ استخدام شركات السيارات
49، 54

جي بي مورغان تشايس 181، 450
جي ميل 43، 56، 67، 88، 100، 105،
120، 137، 201، 202، 220، 229،
310، 411، 325، 459

- ح -

حجب 135، 150، 151، 152، 167،
471؛ حجب ذاتي 151، 152؛ الحد
الأدنى الضروري 242
حركة «احتلوا وول ستريت» 136، 311،
405، 499
حرية الإنترنت 167، 168، 442، 453،
467
حزب القراصنة («هاكرز») في أيسلندا
474

262، 265، 285، 286، 287، 295،
297، 371، 377، 384، 461، 463،
481؛ نظام «جي بي إس» 28، 48، 123
تخطيط بالـ «ويب» 171، 174
تركيا 127، 363، 417، 424
ترومان، هاري 106، 340
تزوير بطاقات الائتمان 211، 462
تسارنارييف، تامرلان 115، 128
تسويق مباشر 90؛
تشفير 121، 137، 138، 140، 141،
185، 186، 188، 275، 310، 380،
395، 486، 498، 499، 501، 502؛
تشفير بطريقة «بي جي بي» 320، 321؛
تشفير تطبيقي [كتاب] (شانير) 186،
452؛ تشفير، «أبواب خلفية» 187، 227،
255، 274، 486
تشويس بوينت 130، 420
تعرف إلى الوجه، تقنية مؤتمتة 48، 148،
207؛ تعرف إلى هوية مغلقة 74
تعمية 244، 323
تعهد بشأن تأثير الخصوصية 296
تقارير، النشاطات المشبوهة 463؛ تقرير
الأقلية 156، 378
تقرير لجنة 9/11 464
تقنيات تعزيز الخصوصية 319، 501
تورش كونسبتس 130
تورلا 120، 411
توم-سكايب 117
تويتر 28، 60، 75، 93، 100، 108،
120، 148، 160، 283، 298، 310،
372، 380، 394، 395، 397، 429،

دبي 50، 75، 375، 386، 423
 درايك، توماس 159، 370
 درون 15، 47، 53، 70، 149، 323،
 368، 373، 376، 430؛ درون هليكوپتر
 47، ميكرو «درون» 53، 70، 373
 دستور الولايات المتحدة، التعديل الأول
 283، 439، 483؛ التعديل الرابع 113،
 256، 263، 477، 484؛ شرعة الحقوق
 344، 509
 دويل كليك 83
 دوكتورو، كوري، 323، 354، 485
 دونت تراك مي 85
 ديبو، هوم 172، 181، 450، 451

- ر -

راترز 183
 رادار 369، 377
 رقابة الحكومة 19، 45، 107، 129،
 151، 188، 277، 278، 308، 321،
 326، 328، 330، 350، 416، 419،
 439؛ الرقابة الشاملة (الكلية القدرة)
 154، 342؛ رقابة الشركات 329؛ الرقابة
 الموجهة 215، 216، 221، 269، 280،
 337؛ رقابة «وكالة الأمن القومي» 276،
 438، 487؛ رقابة بالحوارزميات 200،
 295؛ رقابة عامة 19، 51، 116، 215،
 216، 239، 262، 270؛ رقابة مؤتمتة 55
 رقاقة «رفيد» لا سلكية 53، 332، 376
 روبنز، بلايك، 165، 476
 روبوتكس، (روبوت، علوم) 94
 روزفلت، فرانكلين 340

حضر نووي (دن أ) تركية 32، 387
 الحملات السياسية 93، 393، 450؛
 حملات تصيد 146
 حوسبة السحاب 101، 140، 188،
 189، 190، 192، 328، 329، 397،
 453؛ حقوق المستهلك، 101، رقابة
 الحكومة، 114، 190، 329، مواد تدين
 أمام القضاء 103، «خطأ» تغيير التعريف
 147، «درون» الضربات والرقابة العامة
 15، 70، 149، 323، 368، 373، 376،
 430.

- خ -

خصوصية 16، 88، 151، 188، 191،
 193، 196، 238، 253، 282، 289،
 290، 297، 311، 319، 328، 341،
 421، 443، 455، 490، 492، 494،
 495، 496، 502، 503
 خليوي، ميتا داتا 34، 251
 خليوي، هواتف 12-15، 32، 52، 64،
 114، 158
 حوارزميات 20، 187، 200، 203

- د -

داتنشارشز امكايت (اقتصاد البيانات)
 298، 493
 دافي، تيم 337
 داك داك غو (محرك بحث) 192، 318،
 379، 456
 دالاي لاما 120
 دانيال، جون 160

19، 45، 107، 129، 151، 188، 277،
 278، 308، 321، 326، 328، 330،
 350، 416، 419، 439
 سمات فلتر 135
 سياسة المعلومات 393، 420
 سميث، مايكل لي 113
 سنسنبرينر، جيم 262
 سنودن، إدوارد 5-6، 19، 39، 71،
 105، 109، 112، 121، 123، 127،
 129، 138، 153، 157، 159، 160-
 161، 188، 190، 192، 201، 222،
 225، 228، 231-232، 241، 244،
 253، 260، 264، 267، 273، 308،
 322، 332، 345، 351، 354، 364،
 370، 372، 384-385، 399-400،
 402، 412، 415، 417، 419، 426-
 427، 435، 437، 438، 441-442،
 453، 455، 466، 469، 471، 482-
 484، 487، 499، 509، 510؛ بريد
 إلكتروني 411؛ "قانون التجسس" 159؛
 شهادة أمام البرلمان الأوروبي 482؛ وثائق
 "وكالة الأمن القومي" و"القيادة الحكومية
 للاتصالات" 413، 483
 سواير، بيتر 244، 354، 364، 475
 سوتومايور، سونيا 151، 484
 سورم [كلمة روسية] ("نظام الإجراءات
 لعمليات التحقيق") 117، 408
 سوريا 124، 135، 219، 232، 326،
 424؛ اختراق "وكالة الأمن القومي" 190؛
 البنية التحتية للإنترنت 124
 سوفوس 135

روسيا 108، 117-118، 124-125،
 128، 130، 151، 167-168، 207،
 227، 250، 281-282، 318، 326،
 351، 380، 408-409، 418، 489؛
 تسليح سبراني 413؛ إلزامية تسجيل
 الـ«بلوغرز» 151؛ رقابة عامة 116؛ إساءة
 استعمالها من السلطة 248
 روسيف، ديلما 233
 ريد أكتوبر (فيروس) 120
 ريشليو، كاردينال 164
 ريغان، رونالد 110، 340، 405، 479

-ز-

زابا، فرانك 155، 433
 زوكربيرغ، مارك 168، 190، 195، 196،
 442، 454، 456

-س-

ساركوزي، نيكولا 153
 ستازي 20، 44، 372، 433، 505
 ستاكس نيت 125، 206، 226، 232،
 411، 416، 467، 471
 ستاندرد شاترد (بنك) 63
 ستروس، شارلز 199، 368، 445، 456،
 475
 ستغري (نظام رقابة) 114، 158، 251،
 403، 476
 سرقة، 29، 182، 220، 223، 450،
 451، 462، 469
 سرية، رقابة الشركات 19، 44، 89، 131،
 132، 170، 192، 329؛ رقابة الحكومة

سولوف، دانيال 148، 429، 456، 457، 472
 سوفيت (نظام بنكي) 122، 414
 سويني، لاتانيا 77، 377، 387
 سي نت (موقع إلكتروني) 195، 383، 426، 456، 475
 سيارات، سجلات الصندوق الأسود، 29
 بيانات الـ "جي بي إس" 47، 54
 سياسة لا تسأل لا تخبر 295
 سيجنت (استخبارات الإشارات) 475
 سيسك ("مؤسسة أمن الاتصالات في كندا") 71، 385
 سيسكو (سيستيمز) 140، 189، 329
 سيمنز 134
 سينس نتوركس 13، 70

- ص -

صحة 73، 157، 246، 268، 367؛ رقابة
 269؛ خصوصية بيانات الرعاية 290

- ط -

طالب، نسيم 210، 248
 طريق التحرير 166

- ظ -

ظاهرة «الوادي غير الحاذق» 94، 394

- ع -

عبد المطلب، عمر فاروق 216
 العراق 326، 401، 424
 عصفير غاضبة (لعبة)، تقصي البيانات
 المكانية 84
 العصر الرقمي الجديد (كتاب) (شميدت
 وكوهن) 16، 364، 396
 عوض، نهاد 163
 العيون الخمسة، 126، 127

- ش -

شاترفلاي 393
 شامبرز، جون 190، 454
 شامروك 263
 شتاينهافل، كريغ 219
 شرطة 153، 163، 318، 403، 406، 438، 440، 474، 487؛ دائرة الشرطة في
 سان دييغو 244؛ دائرة الشرطة في شيكاغو
 57؛ دائرة الشرطة في نيويورك 377
 شريمز، ماكس 37، 299، 370
 الشفافية 242، 243، 257، 395، 423، 474، 478، 495، 497، 505، 506
 شميدت، إريك 16، 20، 43، 98، 142، 195، 364، 369، 404، 427، 439، 451، 456، 462

- غ -

328، 341، 345، 348، 366، 370-
372، 375، 379، 383، 388-391،
395، 397-400، 403، 411-412،
414، 427، 432، 445، 447-449،
455-456، 459، 469، 490، 494-
495، 497-499، 502، 504، 507-
508؛ نظارة غوغل 32، 50، 72؛ غوغل
آنا ليتكس 84؛ غوغل بلاس (+) 84، 88،
390، 427؛ سياسة الاسم الحقيقي 86،
390؛ رقابة 84، 88، 390، 427؛ غوغل
قسم الترتيب 341؛ مفكرة غوغل 100؛
وثائق غوغل 100؛ ولاء المستخدم 90،
173، تنقيب في البيانات 59، 62، 210،
211، 212، 214، 215، 216، 381،
462، 463، 464؛ القدرة على تخزين
المعلومات 45، 64، 244، 318، 330؛
طلبات الحكومات لما يمتلكه من معلومات
309؛ النتائج المدفوعة للبحث 177؛ تجميع
نتائج عمليات البحث 302، 94؛ تقارير
شفافية 308؛ انظر أيضاً "جي ميل"
غولد سميث، جاك 5، 251، 337، 338،
354، 413، 476، 505، 506
غولدن شورز تكنولوجيا 81
غيتس، بيل 199
غير، دان (خبير إنترنت) 299
غيل، فيصل 163

- ف -

فاريل، هنري 103، 398
فايل فولت 320، 501
فاينشتاين، ديانا 260، 370، 479، 509

الغاردان، 39، 112، 225، 231، 370-
371، 374، 375، 381، 389، 391،
393، 400، 402، 406، 407، 409-
411، 416، 419-، 421-422، 425-
428، 430-431، 436-438، 442،
445، 449-450، 454، 456-458،
461، 463-464، 466-468، 470،
475، 478-480، 485، 487، 497،
500-501، 504-505، 507، 510؛
نشر وثائق سنودن 39، 112، 225
غازات الدفيئة، انبعاثات 33
غاما غروب 133، 422
غرايسون، آلن 260، 479
غرندر 380
غرينوالد، غلين 39، 370، 371، 375،
381، 382، 400، 417، 418، 426،
436، 440، 466، 469، 478، 487،
497
غفور، عاصم 162
غندي، أوسكار 174، 379، 445
غور، آل 92، 341، 392، 448
غوست نت 120، 411
غوغل 6، 14، 16، 20، 31-32، 36،
42-44، 50، 56، 67، 72، 77، 83،
84-86، 88-89، 94-96، 98-100،
103، 108، 113، 119، 121، 129،
137، 140-142، 153، 174، 177،
178-180، 191، 195، 201-202،
220، 229، 271، 293، 298-299،
302، 307-312، 318-320، 325

18، 31، 45، 56، 63، 70، 79، 82،
90، 104، 106، 108، 110، 118،
163، 265، 287، 288، 294، 295،
298، 312، 327، 401، 443؛ تلاعب
في التدوينات 179؛ سياسة الاسم الحقيقي
390، 86
فيلم "تقرير الأقلية" 156، 378
القاعدة (تنظيم) 107

- ق -

قانون الممارسات العادلة في المعلومات
290؛ قانون أمن الكمبيوتر 280، 489؛
قانون باتريوت، 110، 165، 260، 261،
262، 309، 328، 337، 403، 441،
480، 481، 498، 505
قانون بوزيه كوميتاتوس 279، 488؛
قانون تنظيم سلطات التحقيق (المملكة
المتحدة) 264، 480؛ قانون حماية أميركا
402؛ قانون مراقبة الاستخبارات الأجنبية
(«فيسا») انظر أيضا «قانون تعديلات فيسا»
482؛ قرار بشأن الخصوصية الرقمية 270،
432؛ قوانين نقل الأموال 63
قوى إنفاذ القانون 257، 260، 270،
274، 275، 279، 280، 309، 326،
330، 336، 375، 419، 420، 441،
452، 483، 506؛ إساءة استعمال السلطة
406، 248، 347؛ أي أم إس إي كاتشرز
114، 251، 403؛ البيانات المكاثرة 105؛
عسكرة 487؛ خوارزميات التوقع استعمال
243؛ عنصرية 149؛ سرية 324؛ شفافية
308، 256

فت بت 175، 446
فرنسا 111، 116، 127، 150، 274،
276، 313، 328، 407، 419، 433؛
رقابة الحكومة 151، 277، 328، 419؛
فرانس تليكوم 130
فرومكين، ميخائيل 296، 493
فريزون، 85، 112، 263، 309، 370،
375، 432، 497؛ تقارير شفافية 308
فرينت 486
فرييه، لويس 452
فقاعة الـ«فلتر» 179، 449
فلاش بلوك 86، 319
فلاش كوكيز 85
فلايم 120
فن فيشر 133
فودافون 130، 229، 407، 419
فور تينت 135، 425
فوردر 54
فورستر (مركز بحوث) 189
فوكس-آي تي 120
فيجيلانت سوليوشنز 49
فيرغسون، ولاية «ميزوري»، 244، 469،
475، 508
فيروس «حصان طروادة» 183
فيسا (قانون مراقبة الاستخبارات الأجنبية)
110، 258، 259، 260، 262، 263،
264، 266، 267، 372، 384، 399،
435، 478، 481، 482
فيسبوك، «أعجبنني» («لايك») 56، 67؛
رسم خرائط العلاقات 66؛ قاعدة بيانات
عن تذييلات الصور 56؛ جمع المعلومات

كوميبيوتر 11، 14، 17، 20، 29-30،
 45، 62، 65، 74، 77، 91، 106، 119،
 120، 121، 133، 139، 141-142،
 166، 175، 183، 185، 187، 189-
 190، 202-203، 207، 217-218،
 222، 231، 233، 280-281، 295،
 308، 322، 363، 365، 387، 411-
 413، 440، 443، 451، 458، 466،
 471، 474-475، 489، 493، 494؛
 الهواتف الذكية بوصفها 32، 50، 81،
 121، 304، 366، 452 (انظر أيضاً:
 أجهزة إلكترونية)
 كومسك 250
 كومكاست (شركة)، 85، 99، 397،
 498، 503؛ بوصفها سمسار معلومات
 85، 498، 503
 كونستلر، جايمس 307
 كونغرس، الولايات المتحدة 137، 146،
 158، 159، 162، 214، 226، 253،
 256، 259، 260، 261، 262، 264-
 265، 297-298، 337، 351، 402،
 404، 425، 436، 450، 464، 478،
 479، 482، 484، 488، 493، 505؛
 الإشراف على "وكالة الأمن القومي"
 505؛ قوانين الخصوصية 202، 297،
 447، 491؛ السرية 146
 كوهن، يارد 16، 364
 كوينتيلبرو 162، 163
 كيث، ألكسندر 481
 كيري، جون 159، 437، 477
 كيندل 51، 102، 398

القيادة الحكومية للاتصالات 406، 407،
 419، 473، 481، 485، 510؛

- ك -

كارنيغي-ميلون (جامعة) 394
 كالاها، ماري إلين 247
 كاليا (محكمة) 137، 186، 274
 كاميرن، ديفيد 330، 337
 كريبتوكات 320
 كريدو موبايل 309
 كريدي سويس (بنك) 63
 كريستي، كريس 161، 438
 كريستف كلاود 102
 كلاير، جايمس 201، 370، 459، 477
 كلاين، مارك 370، 419
 كليبر شيب (رقاقة) 186، 187، 188،
 452
 كليتون، بيل 186
 كليتون، هيلاري 159، 167، 442، 445
 كندا، الشراكة الدولية في الاستخبارات
 126
 الكنيسة التوحيدية الأولى 145، 447
 كوالكوم 189، 454
 كوانتوم برنامج «حقن الحزم الرقمية» 231،
 470
 كوبهام 14، 363
 كود بينك (منظمة نسوية) 164
 كوريا الشمالية 125، 326؛ هجمات سبرانية
 125
 كوكيز (ملفات تعريف الارتباط) 83، 84،
 85، 86، 323

ماينغ، تشيلسا 159
مايكروسوفت 27، 70، 85، 100،
103، 108، 118-119، 129، 139،
199، 228، 274، 308-312، 317،
320، 328، 383-385، 389، 397،
426، 432، 447، 467-469، 488،
492، 497-498، 501، 503، 510؛
مايكروسوفت أوفيس 102؛ ولاء المستهلك
173؛ طلبات الحكومة للمعلومات 142؛
تقارير الشفافية 497
مبادرة قومية شاملة لأمن الفضاء السبراني
404
متصفح الإنترنت 103، 319، 331؛
برامج صد الـ«كوكيز» 83، 85، 86،
323؛ متصفح الإنترنت «تور» 240-
241، 321، 324، 381، 411، 461،
466، 470، 473، 502
مجازفة، نفور الدول (الشرطة) 244
مجتمع الاستخبارات الأميركية 112، 213؛
ميزانية 132؛ الخوف 152؛ متعاقدون
من القطاع الخاص 245، سياسة «الباب
الدوار» 133، انظر أيضاً وكالات محدّدة
مجلة وايرد 186، 364، 365-370،
372، 381-382، 389، 395، 397،
400، 402-404، 406، 408، 412،
415، 421، 423، 430، 435، 438،
452-453، 461، 465-467، 470-
471، 473، 476، 484، 486، 499،
502، 505-506، 508

كينزي، ألفرد 77
كينغ، مارتين لوثر 155، 162، 164،
351، 510؛ هوفر، محاولة استغراز 164

-ل-

لافابيت 138، 311، 499
لانيير، يارون 301، 494
اللجنة الفيدرالية للاتصالات 297
اللجنة الفيدرالية للتجارة 82، 177، 183،
297، 377، 388، 447
لجنة مجموعة ماساشوستس للضمان 387
لفيزون، لادار 138، 139
لوك، جون 313، 315، 419، 440،
447، 500
لولزسيك (حركة «هاكرز») 74
لي سميث، مايكل 113
ليبيا 135، 326، 363
ليندو 174، 176

-م-

ماريجوانا 154
مارينا 64
ماسحات ضوئية للوحات المركبات 458
ماسك (فيروس) 120، 121
ماغنا كارتا 312، 313، 315، 500
ماغنا كارتا، نسخة للعصر الرقمي 312،
315
ماك، عناوين 53، 100، 173، 391،
444، 504
ماكونيل، مايك 133
ماكينون، راشيل 315، 390، 500، 501

المعهد الوطني للمعايير والتكنولوجيا
(نيسيت) 280
مغالطة السرد 210، 461
مفتاح المتعهد 187، 452
المفوضية العليا لحقوق الإنسان في الأمم
المتحدة 153
مكاتب الائتمان بوصفها سياسة معلومات
393
مكارثي، إدغار 162
مكارثية 63، 340، 347
مكتب إدارة الموارد البشرية، الولايات
المتحدة 122
مكتب الإحصاء السكاني الأميركي 295
مكتب البحرية للتحقيقات الجرمية 431
مكتب التحقيقات الفيدرالية («إف بي آي»)
45، 48، 49؛ قانون «كاليا» 137، 186؛
برنامج «كويتلبرو» 162-163؛ تكلفة
الرقابة 48؛ مكافحة الإرهاب بوصفها
مهمة 116، 158، 210، 213، 216،
276، 277، 280، 338، 347، 405،
406، 439، 463؛ التنقيب في المعلومات
211-212، 265؛ التبعية بواسطة الـ«جي
بي أس» 151، 373؛ البيانات التاريخية
المخزنة 65، 69؛ التجسس غير الشرعي
45، 263، 406، 473، 486؛ استخدام
«آي أم سي أي كاتشر» 114، 251؛
التجسس الشرعي 113، 452؛ أميركيين
مسلمين مراقبين 107، 163، 406، 440؛
قانون باتريوت 261؛ طلب قواعد البيانات
من شركات الهواتف 166، 202، 311،
397؛ رقابة الاتصالات كلها بوصفها

مجلس الشيوخ الأميركي 161، 201،
260، 263، 266، 337، 377، 391-
392، 439، 480
مجموعات الأخبار 185
محامون 152، 261، 305، 478، 479؛
رقابة الحكومة 152
محركات البحث، نموذج الأعمال 86، 87،
97، 142، 177، 192، 306، 307،
328
المحكمة الأميركية العليا؛ نظام الطرف
الثالث 271
محكمة العدل الأوروبية 132، 302، 329
مذكّرة قضائية 270، آلية الحصول على
270، الدستور 270، «أف بي آي» 270،
تهرب «وكالة الأمن القومي» 270، نظام
الطرف الثالث 271
مراكز الانصهار 116، 405
مركز «بيو» للبحوث 152
المركز الوطني لمكافحة الإرهاب 115
مركز بحوث فورستر 189
مسجل للوحة المفاتيح 47
مسؤولية الثقة المرجعية 305، جمع
المعلومات 307
مشاركة المعلومات مع الاستخبارات
الأميركية 128، 134، 418، 442
مطلقو صفارة الإنذار 159، 259، 268،
269، 330، 419، 441، 466، 483،
484
معدات ذكية 185
معدل الخطأ، التنقيب في البيانات 211
معلومات جينية 57، 60، 63

- هدفاً 136، 382، 452، 468؛ رقابة من
دون مذكرات قضائية 112-114، 261،
277، 362؛ تنصت 46، 138، 187،
258، 274، 468
مكتب الكحول والتبغ والأسلحة 115،
404
مكتب الوثائق 462-463
المكتب الوطني لاعتراض الموجات 99
مكتبة الكونغرس 298، 493
المملكة العربية السعودية 14، 126، 262،
281، 363، 424
المملكة المتحدة 49، 70، 130، 131،
149، 166، 418، 480
منظم حرارة، ذكي 31
موافقة المترابطين شبكياً (ماكينون) 390،
501
موري، ماساهيرو 94
موغلين، إيبين 152، 431، 457، 501
مونزيغر، هكتور 74
ميتادانا 34، 40، 42-44، 64، 213،
365، 371-372، 381-382، 432
463
ميتنيك، كيفن 181
ميركل، أنغيلا 233، 244-245، 276-
277، 418، 472، 475، 487
مينارت 263
ميهانغوس، لويس 183
- ه -**
- هاريس، استطلاع رأي 152
هاريس، كوربوريشن 114، 134
هاكينغ تيم 122-123، 133-134،
414، 423
- ن -**
- نابوليتانو، جانيت 247
ناش (جون) نقطة التوازن 269، 350

وزارة الأمن الوطني 49، 113، 338،
374، 377، 388، 405، 429، 462،
464، 507
وزارة العدل الأميركية 381، 385، 404
وكالة الاستخبارات المركزية (سي آي إيه)
112؛ فاس-سي آي إيه 15؛ في عمليات
الرقابة داخلياً 223
وكالة الأمن القومي، توسيع مهمة 106،
156، 262، 276، 364، 399، 401؛
تعريف فضفاض، 110، 147، 339،
429؛ مخاطر نسبية 20، 209، 254،
241، 257، 330، 473؛ إيغور 326،
418؛ فرادة، 214
وول ستريت جورنال (صحيفة) 172،
361-363، 366، 369، 375، 378،
380، 383، 389-390، 392، 404،
409، 417، 423-424، 432، 435،
439، 444، 446، 452-454، 472،
480-481، 492، 498، 509
ويندوز 108، 120، 173، 317، 484

- ي -

ياهو 96، 103، 119، 129، 139-
140، 179، 308-311، 397، 399،
426، 432، 447، 497، 498-499
يوتيوب 74، 88، 98، 459، 469
اليونان 251، 276

هايدن، مايكل 44، 226، 246، 476
هجمات الإرهاب 337، 339؛ الهجمات
الصينية السبرانية 123
هجمات منع الخدمة 125
الهند 118، 124، 167، 232، 276،
409-410، 420، 424، 442
هواوي (شركة) 123-124، 141، 274،
329، 415
هوبز، توماس 313، 315، 500
هوفر، ج. إدغار 164
هوية 30، 74، 77، 119، 125، 163،
196، 205، 207، 257، 288، 307،
314، 321، 387-388
هيل، راكيل 77
هولت باكارد 175
هيومن رايتس ووتش (منظمة) 118،
152، 428، 432، 483، 500
هيئة الإشراف بصدد الخصوصية والحريات
المدنية 265-266، 481-482

- و -

واتس، بتر 197
واتسون، سارة م.، 354، 380، 395،
495، 501
واي-فاي 15، 56
وايدن، رون 259، 459، 479، 481
وايز 298، 423
وثيقة حقوق الخصوصية 301-302
ورمر (هاكر) 75



